U.S. Department of Energy
Office of River Protection
Contract Management Division
Mr. Michael K. Barrett
Contracting Officer
P.O. Box 450, MSIN H6-60
Richland, Washington 99352

CCN: 033132

Dear Mr. Barrett:

CONTRACT NO. DE-AC27-01RV14136 – TRANSMITTAL FOR APPROVAL: AUTHORIZATION BASIS CHANGE NOTICE 24590-WTP-ABCN-ESH-01-001, REVISION 1, "REVISION TO ISM PROCESS & DEFENSE IN DEPTH (SRD) APPENDICES A & B"

References:
1) CCN 034367, Letter, R. C. Barr, OSR to R. F. Naventi, BNI, "Acceptance of Closeout Comments Associated with the Standards Approval Package Submittal," 02-OSR-0218, dated May 22, 2002.

2) CCN 032382, Letter, R. C. Barr, OSR to R. F. Naventi, BNI, "Response to Early Approval Requests for Certain Authorization Basis Change Notices (ABCN)," 02-OSR-0169, dated April 22, 2002.

3) CCN 030540, Letter, R. C. Barr, OSR to R. F. Naventi, BNI, "Office of Safety Regulation (OSR) Questions on Low Activity Waste Construction Authorization Request and Related Submittals," 02-OSR-0109, dated, March 14, 2002.

4) CCN 026385, Letter, A. R. Verlup, BNI, to M. K. Barrett, ORP, "Transmitted for Approval: Contract Deliverable 'Revised Standards Approval Package' and Associated Authorization Basis Change Notices in Support of the 'SRD Standards Approval Package Submittal,'" dated January 15, 2002.

Bechtel National, Inc. (BNI) is submitting the Authorization Basis Change Notice (ABCN), 24560-WTP-ABCN-ESH-01-001, Revision 1 (attachment), to the U.S. Department of Energy, Office of River Protection, and the Office of Safety Regulation (OSR) for review and approval. This ABCN incorporates the OSR-approved BNI responses to the OSR review questions as noted in Reference 1.

Approval of this ABCN is requested by July 26, 2002.

 CCN: 033132

An electronic copy of ABCN 24590-WTP-ABCN-ESH-01-001, Revision 1, is provided for the OSR's information and use.

If you have any questions or comments, please contact Mr. Bill Spezialetti at (509) 371-4654.

Very truly yours,

A. R. Veirup
Prime Contract Manager

TR/es

Attachment: Authorization Basis Change Notice 24590-WTP-ABCN-ESH-01-001, Revision 1, plus attachments

cc: Name (ALPHABETIZE)	Organization	MSIN
Barr, R. C. w/a (1 hard copy and 1 electronic copy)	OSR	H6-60
Beranek, F. w/o	WTP	MS6-P1
Betts, J. P. w/o	WTP	MS4-A1
Dickey, R. w/o	WTP	MS6-R1
DOE Correspondence Control w/a	ORP	H6-60
Erickson, L. w/o	ORP	H6-60
Gibson, K. w/a	WTP	MS6-R1
Naventi, R. F. w/o	WTP	MS4-A1
PDC w/a	WTP	MS5-K.1
QA Project Files w/a	WTP	MS4-A2
Ryan, T. B. w/a	WTP	MS6-R1
Schwier, J. F. w/o	ORP	H6-60
Struthers, D. J. w/o	ORP	H6-60
Swailes, J. H. w/a	ORP	H6-60
Taylor, W. J. w/a	ORP	H6-60
Veirup, A. R. w/o	WTP	MS4-A1

0127355,17E
24590-WTP-ABCN-ESH-01-001

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-01-001 Revision 1

ABCN Title Revision to ISM Process & Defense in Depth (SRD Appendics A & B)

I. ABCN Review and Approval Signatures

A. ABCN Preparation

Preparer:	A. Hosler		
	Print/Type Name	*Signature*	*Date*
Reviewer:	J. Hinckley		
	Print/Type Name	*Signature*	*Date*

B. Required Reviewers

Review Required? *For each person checked Yes, that signature block must be completed.*

☒	ES&H Manager	Fred Beranek		
		Print/Type Name	*Signature*	*Date*
☒	QA Manager	George Shell		
		Print/Type Name	*Signature*	*Date*
☒	PSC Chair	Bill Poulson		
		Print/Type Name	*Signature*	*Date*
☐	Operations Manager			
		Print/Type Name	*Signature*	*Date*
☐	Engineering Manager			
		Print/Type Name	*Signature*	*Date*
☐	Pretreatment APM			
		Print/Type Name	*Signature*	*Date*
☐	LAW APM			
		Print/Type Name	*Signature*	*Date*
☐	HLW APM			
		Print/Type Name	*Signature*	*Date*
☐	BOF APM			
		Print/Type Name	*Signature*	*Date*
☐	Construction Manager			
		Print/Type Name	*Signature*	*Date*
☐	Business/Project Controls Manager			
		Print/Type Name	*Signature*	*Date*
☐	ALARA PSC Subcommittee Chair			
		Print/Type Name	*Signature*	*Date*
☒	PMT Chair	Dennis Klein		
		Print/Type Name	*Signature*	*Date*

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-01-001 Revision 1

ABCN Title Revision to ISM Process & Defense in Depth (SRD Appendics A & B)

C. ABCN Approval

WTP Project Manager Ron Naventi

Print/Type Name *Signature* *Date*

II. Description of the Proposed Change to the Authorization Basis

D. Affected AB Documents:

Title	Document Number	Revision
Safety Requirements Document, Volume I	24590-WTP-SRD-ESH-01-001-01	0
Safety Requirements Document, Volume II	24590-WTP-SRD-ESH-01-001-02	0
Integrated Safety Management Plan	24590-WTP-ISMP-ESH-01-001	0

Decision to Deviate ☐ Yes ☒ No

If yes, DTD Number Deficiency Report Number

Initiating Document Number Contract No. DE-AC27-01RV14136 Revision

E. Describe the proposed changes to the Authorization Basis Documents:

For SRD Volume I – cancel in its entirety. Previous revisions will exist for historical purposes.

For SRD Safety Criterion 3.1-7 replace the implementing standard ISMP 3.3.3, *Changes to Safety Documentation* and ISMP 5.6.2, *Updating of the Hazard Analysis Report* with 24590-WTP-SRD-ESH-01-001, Appendix A, *Implementing Standard for Safety Standards and Requirements Identification.*

The following changes are proposed for SRD Volume II, Appendix A, revision 0:

1. Add requirements for evaluation of chemical and direct radiation hazards,
2. Change the format of the standard to more closely follow the sequential steps of the ISM process,
3. Revise the presentation of common mode and common cause failures,
4. Delete the requirement that controls for SL-2 events satisfy the single failure criteria,
5. Replace details on SSC classification and quality attributes with references to SRD SC 1.0-8 and the QAM,
6. Editorial and wording changes to more clearly describe the standards selection process. A detailed identification of each proposed change for Appendix A is included in the attached Table 1.
7. Add new section 11.0, Maintenance of the SRD. Change Sections 11.0 and 12.0 to 12.0 and 13.0 respectively.
8. Add new figure A-1, SRD Compliance Process.
9. In Section 4.3.1 identify what facility features can and cannot be credited when assigning Severity Levels

The following changes are proposed for SRD Volume II, Appendix B, revision 0:

1) Add requirements for evaluation of chemical and direct radiation hazards,
2) For SL-1 events in Table 1 state that the single failure criterion shall be applied to the set of two or more barriers credited for meeting exposure standards.
3) For SL-2 events state that the application of the single failure criterion may be required of prevention or

ABCN Number 24590-WTP-ABCN-ESH-01-001 Revision 1

ABCN Title Revision to ISM Process & Defense in Depth (SRD Appendics A & B)

E. Describe the proposed changes to the Authorization Basis Documents:

mitigation controls to meet the target frequency.

For SRD Volume II, Appendix D, revision 0 it is proposed to revise section 2.0, seventh paragraph, 2nd sentence to "The binning process assigns postulated events to a certain severity level for further detailed analysis and comparison to Radiation Exposure Standards".

For ISMP Section 1.3.8 delete the discussions of the performance of process hazards analyses.

The following change is proposed for ISMP Section 3.1, revision 0: Section 3.1.1 will be deleted entirely and Section 3.1 will include the following single sentence "Application of defense-in-depth for the RPP-WTP is provided in Safety Requirements Document (SRD) Volume II, Appendix B, "Implementing Standard for Defense in Depth."

For ISMP Sections 3.6.3 and 3.7.2 it is proposed to reference SRD Volume II, Appendix A instead of ISMP Section 3.1, "Defense-in-Depth".

For ISMP Section 3.7 it is proposed to delete the reference to SRD Volume I, Section 3.4.2 and add the sentence from SRD Volume I, Section 3.4.2.

For ISMP Section 4.2 it is proposed to delete the second paragraph in its entirety.

For ISMP Section 7.4 it is proposed to reference SRD Volume II, Appendix A instead of SRD Volume I, Section 3.6, "SRD Maintenance".

F. List associated ABCNs and AB documents:

The affected sections of the SRD that would be changed by this ABCN are SRD Volume I (cancelled in its entirety), Appendix A of Volume II, "Implementing Standard for Safety Standards and Requirements Identification," SRD Volume II, Appendix B, "Implementing Standard for Defense in Depth," SRD Volume II, Appendix D, "Radiological Exposure Standards for the RPP-WTP Project" and SRD SC 3.1-7. The changes that are common to Appendices A and B are those dealing with application of the single failure criteria and the addition the requirements for direct radiation and chemical release events. The affected parts of the ISMP are Sections 1.3.8 and 3.1.1. Editorial changes are also proposed for ISMP Sections 3.6.3 and 3.7.2 to provide a reference to SRD Appendix B (in lieu of ISMP Section 3.1) for the discussion on defense in depth. Editorial changes are proposed for ISMP Section 3.7 to remove the reference to SRD Volume I and add sentence from SRD Volume I. Editorial change is proposed for ISMP Section 4.2 to delete information that is redundant to SRD Volume II, Appendix D.

No associated ABCNs or AB documents are impacted by this ABCN. AB documents (RPP, ISAR, QAM and HAR) are not impacted. ABCN 24590-WTP-ABCN-ESH-01-027 proposes to delete IEEE-603 from Appendix B and ABCN 24590-WTP-ABCN-ESH-02-003 proposes to relocate IEEE-379 from Appendix B to Appendix C.

G. Explain why the change is needed:

Much of SRD Volume I is no longer current as it documents the process used by BNFL to develop the initial issuance of the SRD. The remaining information regarding maintenance of the SRD (Volume I Section 3.6) is better located in Appendix B.

SRD SC 3.1-7 is updated to replace the ISMP with SRD Volume II, Appendix A as the implementing standard to be consistent with the proposed changes to SRD Volume II, Appendix A. See below.

Relative to the above-listed nine types of proposed changes for Appendix A the reasons are as follows:

1) the existing standard is focused on radiological release events and does not establish requirements for chemical and direct radiation hazards and hazardous situations,

G. Explain why the change is needed:

2) the appendix is somewhat difficult to understand and implement as the sequential steps of the ISM process differs from the presentation provided in the appendix (e.g., the role of design basis accident analysis),

3) the changes regarding common mode and common cause failures are to bring the nomenclature into conformance with the terms and definitions currently in general acceptance throughout the risk and reliability community and eliminate confusion as to the actual meaning of "common mode" and "common cause" designations for multiple failure events,

4) the single failure criteria should only be mandated for SL-1 events, it is required for SL-2 event when necessary to meet the target frequency (this proposed change for Appendix A is consistent with SRD Appendix B, Table 1 as it exists today),

5) to decrease the potential for conflicts it is better to describe the SSC classification process in one place,

6) to correct inconsistencies within Appendix A, between Appendix A and B. A reason for each proposed change in Appendix A is included in the attached Table 1.

7) to add the only part of the SRD standard selection process that is not included in Appendix A and to facilitate cancellation of SRD Volume I.

8) Figure A-1, SRD Compliance Process is added for clarity and to facilitate cancellation of SRD Volume I.

9) to make it clear that Severity Level assignments are generally not to take credit for SSCs but that credit may be taken for liquid retention and plate out in the cells when they are not challenged by the event.

Relative to the above-listed proposed three types of changes for Appendix B the reasons are as follows:

1) the existing standard is focused on radiological release events and does not establish requirements for chemical and direct radiation hazards and hazardous situations,

2) to make it clear that the single failure criterion does not need to be applied to each of the two or more barriers,

3) the current statement for SL-2 events that “The single failure criterion shall be considered” is too strong; for SL-2 events the single failure should be adopted when necessary to meet the target frequency,

The change to Appendix D is necessary to be consistent with the process depicted in Appendix A. See Table 3.

The discussion of hazard identification and binning is proposed for deletion as these processes are addressed in SRD Appendix A, Sections 4.1 and 4.6 respectively. The information on defense in depth contained in ISMP Section 3.1.1 is removed as the appropriate information is now included in SRD Volume II, Appendix B and a few cases in Appendix A. Attached Table 4 of this ABCN identifies information included in ISMP Section 3.1.1 and identifies where it is located in Appendix B. Table 4 also provides justification for those few cases where the information included in ISMP Section 3.1.1 is not included in Appendices A or B. Reference to SRD Volume I is being deleted from the ISMP Section 3.7, since SRD Volume I is being cancelled. The Section 3.7.2 reference to ISMP Section 3.1 for a defense-in-depth discussion is being replaced by reference to Appendix B as the content of Section 3.1 is being removed. The paragraph in ISMP section 4.2 is being deleted as this is redundant to SRD Volume II, Appendix A. ISMP Section 7.4 is being updated to reference SRD Volume II, Appendix A as SRD Maintenance has been added to SRD Volume II, Appendix A, Section 11.0.

ABCN Number 24590-WTP-ABCN-ESH-01-001 Revision 1

ABCN Title Revision to ISM Process & Defense in Depth (SRD Appendics A & B)

H. List the implementation activities and the projected completion dates:

Activity	Date
Inform DOE that AB has been revised	30 days after DOE approval
Distribute revised pages	14 days after DOE approval
Provide updated electronic version of AB to DOE	30 days after DOE approval

Revise the following implementing documents:

	Documents	Describe extent of revisions	Date
1	24590-WTP-GPP-SANA-002, Hazard Analysis, Development of Hazard Control Strategies, and Identification of Standards	Changes to maintain consistency and to state that 10CFR835, Subpart K and F and 10CFR34 include information that may be useful in the identification of administrative controls for direct radiation events.	30 days after DOE approval
2	24590-WTP-GPP-SANA-003, Accident Analyses	Changes to maintain consistency.	30 days after DOE approval

	Describe other activities:	Date
1	N/A	

III. Evaluation of the Proposed Change

I. Is DOE prior approval required?

1 Does the revision involve the deletion or modification of a standard previously identified or established in the SRD? **Yes** ☒ **No** ☐

Explain

SRD Volume II Appendices A, B and D are approved implementing standards for which changes are proposed. Revises SRD SC 3.7-1.

2 Does the revision result in the reduction in commitment currently described in the AB? **Yes** ☐ **No** ☒

Explain

The change does propose removal of commitments relative to classification of SSCs from SRD Appendix A, Section 6.0. However, as these commitments remain in SRD SC 1.0-8, this is not viewed as a reduction in a commitment. The ABCN proposes to delete SRD Volume I. However, commitments in Volume I that apply to the current contract (Section 3.6) are to be relocated to SRD Volume II, Section 11.0, Maintenance of the SRD. The ABCN also proposes deletion of defense in depth discussions from the ISMP Section 3.1.1. Attached Table 4 documents that commitments contained in Section 3.1.1 are addressed elsewhere in the AB.

3 Does the revision result in a reduction in the effectiveness of any procedure, program, plan, or management process described in the AB? **Yes** ☐ **No** ☒

Explain

The change is limited to changes to the AB documents as addressed above.

J. Complete the safety evaluation by describing how the revision to the AB:

1 will continue to comply with all applicable laws and regulations, conform to top-level safety standards, and provide adequate safety

The proposed changes do not impact commitments made relative to laws and regulations (e.g., commitments made to 10CFR820, 830 and 835 are not impacted, also 10CFR1910.119 and 40CFR68 will be implemented if the facility exceeds threshold quantities) or top-level safety standards (in particular, commitments to DOE/RL-96-0004 and –0006 are retained). Commitments to DOE/RL-96-0004 relative to standards selection to achieve adequate safety are retained.

2 will continue to conform to the original submittal requirements associated with the AB documents being revised

The original submittal requirements to define controls that achieve compliance with the exposure standards of SRD Volume II, Section 2.0 for normal events and off-normal events (anticipated, unlikely and extremely unlikely events) and to select standards by a process that complies with DOE/RL-96-0004 are retained.

3 will not result in inconsistencies with other commitments and descriptions contained in the AB or an authorization agreement

Including the proposed changes to SRD Volume II, Appendices A, B, and D and SC 3.1-7 within this one ABCN decreases the potential for inconsistencies between these to portions of the SRD. The replacement of the details on SSC classification and attributes in Section 6.0 of Appendix A with references to SRD SC 1.0-8 and the QAM for these requirements removes the potential of inconsistencies in these discussions.

ISMP Sections that relate to SRD Volume II, Appendices A and B (e.g., 1.3.4, "Process Hazards Analysis." 1.3.6, "Accident Analysis," 4.1, "Safety Management Processes,") do not require changes as a result of the proposed changes to the SRD. It proposed to remove the defense in depth discussion contained in ISMP Section 3.1.1, in part, to eliminate the potential for inconsistencies with SRD Appendix B. The reference to SRD Volume I in ISMP Section 3.7 is being removed, since the SRD Volume I is being cancelled. A paragraph in ISMP, Section 4.2 "Tailoring Safety Management Processes" required a change to remove duplicate information.

The proposed changes to the SRD do not relate to fundamental aspects of the design as described in the ISAR nor to new or significant or bounding hazards not identified in the HAR. The proposed changes are consistent with the RPP (the ABCN does not propose changes relative to the implementation of 10CFR835).

K. Justification of the Proposed Change

Provide a justification that demonstrates that the proposed change is safe

Canceling SRD Volume I, modifying the SRD Volume II, Appendices A, B, and D, revising SC 3.7-1, and modifying the ISMP to remain consistent is safe and does not impact the regulatory basis of DOE/RL-96-0004 and DOE/RL-96-0006 for the standard selection process or defense in depth. Additionally the laws and regulations, commitments made to 10CFR820, 830 and 835 are not impacted (10CFR1910.119 and 40CFR68 will be implemented if the facility exceeds threshold quantities) by the proposed change. Justification for specific proposed changes is provided below:

ABCN Number 24590-WTP-ABCN-ESH-01-001 Revision 1

ABCN Title Revision to ISM Process & Defense in Depth (SRD Appendics A & B)

Provide a justification that demonstrates that the proposed change is safe

1. **It is proposed to cancel SRD Volume I and move section 3.6, SRD Maintenance to SRD Volume II as Section 11.0.** SRD Volume I (except for section 3.6) contains only historical information The historical information will be retained in earlier SRD revisions. The information contained in SRD Volume I, Appendices A, B, C, D & E is no longer current and has not been updated. The Standards Identification Process Database (SIPD) will provide the link for design requirements. The information in Volume I, Section 3.6 on maintenance of the SRD will be moved to Volume II, Appendix A, Section 11.

2. **It is proposed to revise SRD Volume II, Appendix A to allow for credit to be taken for certain features of caves and cells in the assignment of Severity Levels.** Credit can be taken for the liquid retention and plateout the might occur with the cells and caves. These are passive features of the facility that are not challenged by the loadings that may be placed on them by the accident. Credit will not be taken for less robust confinement features such as seals, ductwork, and filters.

3. **It is proposed to add requirements to SRD Volume II, Appendices A and B, for analysis of chemical and direct radiation hazards.** These additions are considered to be safe as the appendices currently provide no requirements for the analyses of such events. Table 2 of Appendix B that addresses Severity Levels for direct radiation events is patterned after existing Table 1 used for radiological release events. Section 5.3 of Appendix A is based upon control of chemical hazards in the commercial process industry but also acknowledges that the WTP may have special conditions that require additional controls.

4. **It is proposed to replace the discussion of Common Mode/Common Cause failure in SRD Volume II, Appendix A, Section 4.5 with a discussion of Dependent Failures.** In the analyses of dependent failures it is not important to know if the failures are internal or external to the systems as the failures are treated the same. This change is to bring the nomenclature into conformance with the terms and definitions currently in general acceptance throughout the risk and reliability community and eliminate confusion as to the actual meaning of "common mode" and "common cause" designations for multiple failure events. This process is consistent with the definitions of common mode and common cause failures included in DOE/RL-96-0006 including the requirements of Section 4.2.2.2 of DOE/RL-96-0006.

5. **SRD Volume II, Appendices A and B will be revised to provide a consistent discussion of SLs 1 and 2 relative to barriers and the single failure criterion (SFC).** For SL-1 events it will be stated that the SFC shall be applied to the set of two or more barriers credited for meeting exposure standards to remove any misunderstanding that the SFC must be applied to both barriers which could lead to quad redundancy with is

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-01-001 Revision 1

ABCN Title Revision to ISM Process & Defense in Depth (SRD Appendics A & B)

Provide a justification that demonstrates that the proposed change is safe

not a requirement of the project. For SL-2 events it will be explained that the SFC may be required to meet the target frequency rather than stating that the SFC shall be considered for SL-2 events. This is to make it clear when the SFC might need to be applied to SL-2 events.

L. Certification of Continued SRD Adequacy

Based on evaluations from III.I.1 and III.J.1. If question III.I.1 is marked "yes, Project Manager certification is required. The Project Manager's signature certifies that the revised SRD continues to identify a set of standards that provide adequate safety, complies with WTP applicable laws and regulations, and conforms with top-level safety standards and principles. This certification is based on adherence to the DOE/RL-96-0004 standards identification process and successful completion of review and confirmation by the PSC.

WTP Project Manager:

Print/Type Name	*Signature*	*Date*

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-01-001 Revision 1

ABCN Title Revision to ISM Process & Defense in Depth (SRD Appendics A & B)

M. List of Attachments:

1. Safety Requirements Document (SRD), 24590-WTP-ESH-SRD-01-001-02, Proposed Changes
2. Integrated Safety Management Plan (ISMP), 24590-WTP-ESH-ISP-01-001, Proposed Changes
3. Table 1- SRD Volume II, Appendix A – Proposed Changes
4. Table 2 – SRD Volume II, Appendix B – Proposed Changes
5. Table 3 – SRD Volume II, Appendix D – Proposed Changes
6. Table 4 – Content of ISMP Section 3.1.1 versus Content of SRD, Volume II Appendix B
7. Revision to Implementing Standard for RPP-WTP ISM Process and Defense-in-Depth

24590-WTP-ABCN-ESH-01-001 Rev 1

Attachment 1

Proposed changes to the *Safety Requirements Document Volume II*

# of pages (including cover sheet): 48

Note: Revision marks in this attachment represent proposed changes to the approved *Safety Requirements Document Volume II*. They do not indicate changes from Revision 0 of this ABCN.

Safety Criterion: 3.1 - 6

A system shall be established to promptly address the hazard analysis team's findings and recommendations; assure that the recommendations are resolved in a timely manner; and that the resolution is documented. The contractor shall document what actions are to be taken; complete actions; develop a written schedule of when these actions are to be completed; communicate the actions to operating, maintenance and other employees whose work assignments are in the process and who may be affected by the recommendations or actions.

Implementing Codes and Standards

BNFL-5193-SRD-01, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

29 CFR 1910 Occupational Safety and Health Standards Location: 119 (e)
40 CFR 68 Chemical Accident Prevention Provisions Location: 50
DOE/RL-96-0006 5.2.2 Process Hazard Analysis

Safety Criterion: 3.1 - 7

At least every five (5) years after the completion of the initial process hazard analysis, the process hazard analysis shall be updated and revalidated by a qualified team, to assure that the process hazard analysis is consistent with the current process.

Implementing Codes and Standards

~~BNFL-5193-ISP-01 Integrated Safety Management Plan~~
~~Section: 3.3.3 Changes to Safety Documentation~~
~~Section: 5.6.2 Updating of the Hazard Analysis Report~~
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

29 CFR 1910 Occupational Safety and Health Standards Location: 119 (e)
40 CFR 68 Chemical Accident Prevention Provisions Location: 50
DOE/RL-96-0006 5.2.2 Process Hazard Analysis

Safety Criterion: 3.1 - 8

Employers shall retain process hazards analyses and updates or revalidations as well as the documented resolution of any recommendations for the life of the process.

Implementing Codes and Standards

BNFL-5193-ISP-01 Integrated Safety Management Plan
Section: 5.5 Process Hazards Analysis
Chapter: 8.0 Document Control and Maintenance

Regulatory Basis

29 CFR 1910 Occupational Safety and Health Standards Location: 119 (e)
40 CFR 68 Chemical Accident Prevention Provisions Location: 50

CONTENTS

1.0 Introduction A-1
2.0 Process Initiation A-1
3.0 Identification of Work A-2
4.0 Hazard Evaluation A-3
4.1 Identification of Hazards A-4
4.2 Identification of Potential Accident/Event Sequences A-4
4.3 Estimation of Consequences A-4
4.3.1 Accident Severity Level Identification A-4
4.3.2 Accident Analysis (this section has been deleted) A-5
4.3.3 Normal Conditions A-6
4.4 Estimation of ~~Accident~~ Event Frequencies A-7
4.5 Consideration ~~of Common Cause/Common Mode~~for Dependent ~~f~~Failures A-7
4.6 ~~Definition~~ Selection and Analysis of Design Basis Events A-8
4.7 Definition of Operating Environment A-8
4.8 Identification of Potential Controls A-8
4.9 Documentation of the Hazard Evaluation A-9
5.0 Development of Preferred Hazard Control Strategies A-10
5.1 Approach for Radiological Release Events A-12
5.2 Approach for Direct Radiation Exposure Events A-13A
5.3 Approach for Chemical Events A-13B
6.0 Classification of Structures, Systems, and Components A-14
7.0 Identification of Standards A-16
8.0 Confirmation of Standards A-18A
9.0 Formal Documentation A-18A
10.0 Recommendation A-18A
11.0 Maintenance of the SRD A-18A
12~~1~~.0 Definitions A-19
13.0 References A-20

1.0 Introduction

This standard implements the process for establishing a set of radiological, nuclear, and process safety requirements and standards as described in DOE/RL-96-0004 and RL/REG-98-17. The Project refers to this process as Integrated Safety Management (ISM).

The activities described below establish radiological, nuclear and process safety standards and requirements for design, construction, and operation of the facility. Establishment of safety standards and requirements (from work identification through confirmation of standards) is an iterative process that takes place throughout the life of the project. ~~As the design evolves, t~~ The process repeatedly evaluates these standards and requirements based on the evolving design. The initial ISM activities may not completely implement all elements of this standard. However, the standard will be completely implemented prior to receiving the Construction Authorization for design and construction issues and the Operating Authorization for design, construction, and operating issues. The appropriate activities for a particular hazard will also be completed (including review and approval by the regulator) prior to receiving the related hazardous material at the RPP-WTP.

The Safety Requirements Document (SRD) provides formal documentation of the standards~~, which are a~~ resulting ~~of~~ from this process. The SRD is updated as ~~required~~ needed to reflect the results of successive iterations of the standards and requirements identification process (i.e., the ISM process).

2.0 Process Initiation

The RPP-WTP Project Manager shall ensure implementation of the Project Management Plan, thus assuring that adequate resources ~~with appropriate technical background~~ are available and organized to perform ~~subsequent~~ the tasks required by this standard. Personnel with appropriate technical backgrounds shall be assigned to the tasks. This activity also assures that the input information required for the safety standards and requirements identification process has been collected and organized. This input information includes the top-level safety standards and principles stipulated by DOE in DOE/RL-96-0006 and the laws and regulations applicable to the RPP-WTP project.

The DOE/RL-96-0004 safety requirements and standards identification Process Manager for the project is the Radiological, Nuclear, and Process Safety Manager.

The Process Manager chairs the DOE/RL-96-0004 safety requirements and standards identification Process Management Team (PMT). The PMT is constituted in accordance with project implementing documents and includes managers from the following project organizations:

- Environmental, Safety, & Health
- Engineering
- Operations

The Process Management Team shall oversee the ISM process and shall provide resources and resolve issues as necessary. The PMT shall set up ~~integrated~~ ISM ~~t~~Teams for the conduct of ISM usually on a plant system basis. During facility operation, the process hazard analysis shall be updated to reflect changes concurrently with the annual update of the FSAR. Individual PMT members shall provide various subject matter experts to help fulfill the roles required of the ~~Integrated~~ ISM Teams for conduct of the ISM process.

3.0 Identification of Work

The aim of this activity is to describe the work that will be performed so that the hazards inherent in the work can be identified and evaluated. Work activity experts who have extensive knowledge of the overall processing approach and are integrally associated with the facility design shall perform this activity. W~~w~~ork activity experts shall be drawn from the following RPP-WTP organizations:

- Engineering staff
- Operations staff

When appropriate, the PMT may also draw work activity experts from the staff of other departments, such as from Construction.

In an overall sense, identification of work involves definition of the project mission and identification of the processes that must be performed to accomplish the mission. It includes selection of optimum functions, processes, and parameters through trade studies and definition of functional requirements. Identification of work for the purpose of design development involves definition of various plant systems, structures, and components. This latter definition is the focus for the ~~Integrated~~ ISM Teams created to conduct ISM on a plant system basis.

The product of this activity includes:

- Process description
- System descriptions
- Descriptions of key structures
- Basis of design documents
- PFDs, MFDs, and P&IDs

~~The results of the identification of work activity shall be documented in the SRD by inclusion or by reference.~~

~~The identification of work activity is an iterative process. Identification of work will be reconsidered in light of design evolution, the outcome of hazard evaluations, and the development of hazard control strategies.~~

4.0 Hazard Evaluation

The aim of the hazard evaluation activity is to identify and characterize the hazards resulting from the work. The ~~integrated~~ ISM ~~t~~Teams shall conduct the hazard evaluation activity usually on a plant system basis. These teams shall include work activity experts (as defined in Section 3.0), hazard assessment experts, and hazard control experts.

Hazard assessment experts and hazard control experts shall generally be members of the technical staffs of the Safety Analysis Manager and of the Regulatory Safety Manager. The process management team shall provide additional technical resources as required to evaluate the hazards.

The hazard evaluation shall address hazards inherent in normal operation as well as potential accidents resulting from abnormal internal and external events.

The hazard evaluation shall comprise the following elements:

- Identification of Hazards
- Identification of Potential Accident/Event Sequences
- Estimation of Accident Consequences
- Estimation of Accident Frequencies
- Consideration of Common Cause and Common Mode Failures
- Definition of Design Basis Events
- Definition of Operating Environment
- Identification of Potential Control Strategies
- Documentation

These elements are discussed below.

4.1 Identification of Hazards

The objective of this element is to systematically identify the hazards associated with the defined work.

The ~~integrated~~ ISM ~~t~~Teams shall compile a list of hazardous materials and energy sources associated with the facility processes, design, and operations. This list shall be compiled based on the identified work. This compilation provides information used to identify potential accidents resulting in the uncontrolled release of hazardous material or energy to facility and collocated workers, the public, and the environment. The team may use checklists to guide the compilation process and to assure that all potential hazards from both natural and manmade sources originating from outside and inside the facility are addressed.

4.2 Identification of Potential Accident/Event Sequences

The objective of this element is to perform a structured and systematic examination of the facility and its operations to identify potential accidents (including those resulting from common mode and common cause failures). The team shall conduct this examination using methodologies and guidelines in AIChE (1992).

4.3 Estimation of Consequences

4.3.1 Accident Severity Level Identification

A severity level, SL, shall be assigned to each postulated radiological accident. The severity level shall reflect the unmitigated consequences of the postulated accident (i.e., should not credit SSCs that prevent or mitigate the release) with the following exception. The severity level assignment may credit the contribution that a cell or cave makes to a leak path factor, to limitation of spilled liquid pool size, or to plateout when the credited aspect of the cell or cave is not challenged by the event. ~~Unmitigated~~ C ~~c~~onsequence estimates supporting severity level assignment shall ~~account for the~~be based on bounding assumptions regarding such factors as quantity, form, leak path, plateout, and location of the radioactive material available for release, and the energy sources available to interact with the hazardous material. ~~Unmitigated consequences shall not account SSCs that serve to prevent or mitigate the release. Specifically, unmitigated~~ Severity level consequence estimates shall be evaluated ~~on the basis of~~ as ground level releases. The severity level shall be defined as follows:

SL	Facility Worker Consequence	Collocated Worker Consequence	Public Consequence
SL-1	> 25 rem/event	> 25 rem/event	> 5 rem/event
SL-2	5 - 25 rem/event	5 - 25 rem/event	1 - 5 rem/event
SL-3	1 - 5 rem/event	1 - 5 rem/event	0.1 - 1 rem/event
SL-4	< 1 rem/event	< 1 rem/event	< 0.1 rem/event

These severity levels are related to the radiological and process standards of SRD Chapter 2.0 as follows:

- The unmitigated consequences associated with SL-1 events exceed the radiological standards for extremely unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-2 events are below the radiological standards for extremely unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-3 events are below the radiological standards for unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-4 events are below the radiological standards for anticipated events (SRD Safety Criterion 2.0-1).

Consequences to the facility worker shall be evaluated at the worst-case occupied location. Consequences to the collocated worker and the public shall be evaluated at the locations specified in Appendix D to the *Safety Requirements Document, Volume II*.

Early in the design, the severity level ~~is~~ estimate may be quantitative analysis or a qualitative assessment~~d~~ based on the experience of the ~~Integrated~~ ISM Teams~~. As the design progresses, these estimates are confirmed through the formal accident analyses described in Section 4.3.2. These accident analyses do not address all of the potential accidents identified, but they do address bounding examples of each type of accident. The team should use the results of the accident analyses to validate the severity level estimates for potential accidents not addressed in the formal accident analyses~~. Assumptions upon which the severity level estimates are based shall be documented and linked by reference to the hazardous situation to which they apply. As the design progresses, early assumptions may be confirmed or replaced by design information. If later design information changes the conclusion of the severity level assessment, the effect of the change on subsequent activities of the ISM process shall be evaluated by the ISM Team.

The potential consequences of releases of hazardous chemicals shall also be assessed. The assessment shall consider both the inherent hazard of the chemical itself, and the potential for the chemical hazard to initiate or exacerbate a radiological hazard.

4.3.2 Accident Analysis (this section has been deleted)

~~Accident analyses provide confirmation that the design satisfies the radiological and process standards in the SRD. Accident analyses also provide confirmation of the severity levels assigned to potential accidents.~~

~~The formal accident analyses shall address design basis external events and natural phenomena as well as postulated internal events.~~

~~The postulated internal events shall be grouped by type. Accident types applicable to the RPP-WTP include the following:~~

- ~~Liquid spills~~
- ~~Spills of solid materials~~
- ~~Pressurized releases~~
- ~~Chemical reactions~~
- ~~Boiling~~
- ~~Flammable gas ignition (e.g., hydrogen in air)~~
- ~~Fires~~
- ~~Load drops~~
- ~~Radiation exposure~~
- ~~Criticality~~

~~As a minimum, the accident analysis shall address the most severe credible event of each type.~~

~~Initially, the accident analysis shall evaluate the unmitigated consequences of the postulated accidents. As control strategies are developed, the accident analysis shall also evaluate the impact of the SSCs that implement the control strategy on the potential consequences.~~

~~The accident analysis shall consider the following factors:~~

- ~~Inventory of material at risk in the scenario.~~
- ~~The respirable release fraction for the accident scenario. This is a function of the composition of the material at risk, of the form of the material, and of the interaction between the material at risk and the energy available in the accident scenario.~~
- ~~The fraction of the airborne material released to potentially occupied locations or the environment.~~
- ~~Bounding atmospheric dispersion coefficients (if appropriate).~~
- ~~Radiological composition of the material released.~~
- ~~External radiation field.~~
- ~~Exposure times.~~

~~The accident analysis shall address the potential consequence to facility workers, collocated workers, and the public.~~

4.3.3 Normal Conditions

Some hazards inherent in normal operation must be mitigated to comply with the standards for normal operation in SRD Chapter 2.0. Such hazards shall be addressed in accordance with the RPP-WTP Radiation Protection Plan.

4.4 Estimation of ~~Accident~~ Event Frequencies

There is normally insufficient information early in the design to accurately quantify the frequency of postulated internal events because this frequency depends on the design of the SSCs that implement the control strategy used to manage the hazard. At an early stage, frequency evaluations may be based on the team's experience with similar hazards in similar facilities. The team shall validate these estimates as the design develops.

As the design matures, information on the frequency of hazardous events ~~is~~ may be gained from the use of hazard evaluation techniques that provide frequency data (~~i.e., HAZOP, FMEA, Event Trees, and Fault Trees~~e.g., event and fault trees). Evaluations of the frequency of failure in redundant systems or in diverse systems using similar equipment shall consider dependent failures.

The frequencies of design basis external events may be derived from existing analyses (e.g., safety analyses for adjacent facilities), from evaluation of historical data (e.g., transportation data), or from site-specific information (e.g., seismic history).

4.5 Consideration ~~of Common Cause/Common Mode~~for Dependent F~~f~~ailures

~~The following are typical common cause events:~~

~~□ Natural phenomena events~~
~~□ External man made events~~
~~□ Loss of electrical power~~
~~□ Fire~~
~~□ Internal missiles~~
~~□ Internal flooding~~

~~Common cause events should be treated as discrete events in the hazard analysis. The analyses of common cause events shall focus on identifying provisions to prevent the loss of safety function. The analyses of natural phenomena events shall consider induced effects, such as fire and loss of electrical power.~~

~~Common mode failures shall be addressed through dependent failure modeling as required by Section 4.4 above.~~Consideration is given to dependent failures which includes what has been defined elsewhere (e.g., DOE/RL-96-0006) as common mode failures (events internal to the system) and common cause failures (events external to the system).

The internal aspects of dependent failures are divided into three broad categories:

1 Internal challenges
2 Intersystem dependencies
3 Intercomponent dependencies

These intersystem and intercomponent dependencies may be further divided into four broad categories:

1 Funtional. For example:

- Process upsets or deviations from the normal operating envelope which challenge multiple components (loss of feed, loss of ventilation, loss of offsite power, loss of cooling).
- Motive power, control or cooling systems which provide functional support to more than one, otherwise independent, system.
- Single components that provide multiple functions.

2 Share equipment. For example:

- Redundant systems which share a single component.
- Redundant trains which share a single header.

3 Physical. For example:

- Extreme environments caused by high temperatures and moisture (steam), fires, internal floods.
- Shared locations where an energetic failure of one component can initiate failure of another nearby component.

4 Human-caused dependencies. For example:

- Operator/maintainer errors causing failure of two or more independent systems.
- Design errors in redundant control systems.

The external aspects of dependent failures include both natural phenomena events and man-made environmental effects which make failures dependent. For example:

1 Natural Phenomena Hazards, e.g., seismic activity, ash fallout from volcanism, high winds, external fires and local flooding.

2 Man-made hazards, e.g., airplane crashes, explosions on nearby transportation routes, and chemical and radiological releases from other facilities.

4.6 ~~Definition~~ Selection and Analysis of Design Basis Events

The hazard evaluation ~~shall identify~~performed by the ISM Team involves the identifcation of internal hazards and hazardous situations leading to the selection of a set of internal design basis events. These design basis events shall be selected to ~~define~~ establish a set of bounding performance requirements for the SSCs relied upon to control the internal hazards and hazardous situations. Analysis of the design basis events also provides confirmation that the design satisfies the requirements of SRD Volume II Safety Criteria 2.0-1 and 2.0-2.

The hazard evaluation shall also select a set of external man made design basis events~~. These events shall be selected~~ based upon ~~the results of the hazard analysis to define~~information provided to the ISM Team on nearby facilities and transportation. These events shall establish a set of bounding performance requirements for the SSCs relied upon to mitigate these external events.

~~The integrated teams perform the identification of internal and external design basis events.~~

Design basis natural phenomena loads shall be as defined in the SRD Volume II Safety Criteria 4.1-3 and 4.1-4.

4.7 Definition of Operating Environment

The hazard evaluation shall define a set of bounding operating conditions in which SSCs relied upon to control hazards must function. Environmental parameters to be addressed include the following:

- Temperature
- Pressure
- Humidity
- Radiation Levels
- Chemical Environment

4.8 Identification of Potential Hazard Control Strategies

Based on the experience and judgement of team members, the ~~integrated~~ ISM T~~t~~eam shall identify ~~an initial set of~~one or more potential hazard control strategies to manage each potential accident (i.e., hazardous situations that may result in unacceptable consequences). This set of potential hazard control strategies shall address means of preventing the potential accident and should address means of mitigating the consequences of the accident. The function(s) of each potential hazard control strategy should be clearly described. Potential hazard control strategies shall be identified to manage accident conditions arising from upsets in the process, conditions arising from external events, and conditions inherent in the normal operation of the process.

4.9 Documentation of the Hazard Evaluation

The results of the hazard evaluation shall be documented in a hazard analysis report (HAR) or a safety analysis report (SAR). The results of the process of conducting the various steps of the hazard evaluation shall be contained or referenced in a hazard database. For each hazard considered, the hazard database shall ~~record~~ record or reference the following information produced by the hazard evaluation:

- Hazard identifier
- Hazard description
- Initiators of the hazardous situation
- Hazard severity level estimate ~~(based on unmitigated consequences)~~
- Basis for the ~~S~~severity level ~~basis~~assignment, including assumptions affecting the estimate

~~Assumptions affecting the release (material at risk, energy available, etc)~~

- Hazard frequency estimate
- Basis for frequency estimate
- Potential hazard control strategies and function~~s~~al requirements
- References for the hazard (these would typically be products of the work identification process)

~~Hazard evaluation documentation shall be included in the SRD by inclusion or by reference~~The HAR or SAR shall also contain information on the performance of the hazard evaluation. This ~~documentation~~ information shall include the following:

- Description of the comprehensive approach to hazard evaluation
- Description of the methodology for identification and quantification of work hazards
- Description of the methodology for identifying potential accident scenarios
- Description of the methodology for consequence assessment
- Clear identification of assumptions (e.g., quantity and form of material at risk, rate of release and relevant process conditions) that may drive or inhibit the potential accident ~~must be clearly identified~~

~~Description of results~~

- Evidence of appropriate staffing, and adequate technical staffing and structure applied to the hazard evaluation

5.0 Development of Preferred Hazard Control Strategies

The aim of ~~the development of control strategies~~this activity is to identify a means of controlling each of the hazards identified in the hazard evaluation. The ~~integrated~~ ISM T~~t~~eams ~~of~~ that include work activity experts, hazard assessment experts, and hazard control experts, as discussed in Sections 3.0 and 4.0, perform this activity.

The PMT members shall provide additional technical resources as required to develop the preferred hazard control strategies.

The ~~integrated~~ ISM T~~t~~eams select preferred control strategies based on the set of potential controls identified by the hazard evaluation team. Selection of the preferred strategy considers the following factors:

- The functions required of the preferred hazard control strategy in order to control the hazard
- The degree of defense in depth and reliability provided by the preferred hazard control strategy. The Implementing Standard for Defense in Depth provides ~~guidance~~ requirements and goals in this area.
- Applicable design basis events.
- The operating environment (e.g., temperature and humidity) in which the SSCs implementing the preferred hazard control strategy must function.
- Effectiveness and efficiency of the preferred hazard control strategy.
- Conformance with the DOE stipulated top level standards.
- Compliance with applicable laws and regulations.

The preferred hazard control strategy should be documented in the SAR and will typically comprise a series of elements including some or all of the following:

- Passive and/or active SSCs that function to prevent the release (that is, SSCs that reduce the probability that a release will occur)
- Passive and/or active SSCs that function to mitigate the release (that is, SSCs that reduce the consequences once a release has occurred)
- Administrative controls (for example, limits on inventory)

Consistent with the defense in depth principle, the control strategy development should emphasize preventive measures. It should also emphasize passive SSCs over active SSCs and retention of released material over dispersion. Ideally, the preferred control strategy should incorporate SSCs that prevent releases and SSCs that mitigate the consequences of a release, should it occur.

Once the preferred control strategy is identified, it shall be evaluated for the most bounding conditions (i.e., the most demanding requirements imposed by the set of hazardous situations that credit the function of the control strategy) using the techniques described in Section 4.3 through 4.5. In addition, the evaluation of the preferred hazard control strategy shall identify the measures necessary to assure that it performs its functions reliably. Such measures include maintenance requirements, testing intervals and calibration frequency. The results of this evaluation serve to confirm that the preferred hazard control strategy is capable of satisfying SRD Safety Criterion~~a~~ 2.0-1.

If credit is taken for operator action to satisfy the public radiological exposure standards of Safety Criterion 2.0-1, adequate radiation protection is provided to permit access and occupancy of the control room or other control locations under accident conditions without personnel receiving radiation doses in excess of 5 rem TEDE whole body gamma and 30 rem beta skin for the duration of the accident. If credit is taken for operator action to satisfy public chemical exposure to ERPG-2 limits, provisions for operational access and control are made so that the operator exposure does not exceed the ERPG-2 limits.

Documentation of the hazard control strategy development process shall clearly indicate selection of the preferred hazard control strategies and show the linkage of the control strategies to the respective hazards. The preferred control strategy should be described in terms of the safety functions required (e.g., limit release of radionuclides, etc.) and in terms of a set of engineered features, administrative controls (procedures and training), and management systems selected for implementing the strategy. When the nature of the hazard or hazardous situation is such that the appropriate preferred hazard control strategy is self-evident, the documentation need only demonstrate that the control strategy meets most, if not all, of the selection criteria, and need not provide a discussion of other, nonapplicable control strategies. Similarly, where a proven preferred hazard control strategy that is appropriate to the hazard exists and it is obvious to the team that there are no other alternative control strategies that could be equally attractive, then the documentation need only demonstrate that the control strategy meets most, if not all, of the selection criteria. Otherwise, the documentation should identify all control strategies considered and provide a defensible rationale for selection of the preferred strategy.

The following information produced by the preferred hazard control strategy definition shall be recorded in the hazard database:

- Preferred hazard control strategy
- Linkage of the preferred hazard control strategy to the respective hazards
- Rationale for preferred hazard control strategy selection
- Defense in depth provided
- Control strategy functions and performance requirements
- Estimate of the unmitigated event frequency
- Estimate of the consequences from the mitigated event (by performance of the Design Basis Event [DBE] analysis)
- Estimate of the mitigated event frequency (by performance of the DBE analysis)
- Applicable design basis events (e.g., design basis earthquake)

One of the issues in developing a preferred hazard control strategy for a particular hazard or hazardous situation is determining the number of layers of prevention and mitigation appropriate for the hazard. The preferred hazard control strategies shall conform to the requirements defined in the Implementing Standard for Defense in Depth. In addition, the following guidance shall be considered in developing preferred hazard control strategies.

5.1 Approach for Radiological Release Events

The general RPP-WTP design approach is to provide two confinement barriers against the release of ~~hazardous~~ radiological materials. The process vessels and piping usually form the primary confinement barrier; the process cells and associated ventilation system usually form the secondary confinement barrier. Releases from the primary confinement are mitigated by the secondary confinement.

The accident severity levels defined in Section 4.3.1 are related to the exposure standards in SRD Safety Criterion 2.0-1. The SRD Safety Criterion 2.0-1 exposure standards are frequency based, so it is possible to establish target frequencies for events with a given severity level. The target frequencies tabulated below are consistent with SRD Safety Criterion 2.0-1.

SL	Event Target Frequency (yr^{-1})
SL-1	$<10^{-6}$
SL-2	$<10^{-4}$
SL-3	$<10^{-2}$
SL-4	$<10^{-1}$

These target frequencies may be used to guide control strategy development as described below. In all cases, the control strategy development must conform to SRD Safety Criterion 2.0-1.

For SL-1 events:

- ~~Meeting the target frequency will usually require a control strategy that incorporates diverse and independent SSCs that act to prevent and mitigate the event~~Systems and components credited for meeting exposure standards shall satisfy the single failure criterion as discussed in the Implementing Standard for Defense in Depth (SRD Volume II, Appendix B). The independence and/or diversity that this requires will assist in meeting the target frequency for SL-1 events.

~~Meeting the target frequency will usually require diverse SSCs that act to prevent the release.~~

- The degree of mitigation required depends on the release frequency, that is, on the reliability of the preventive SSCs. For example, assume that the preventive SSCs assure that the frequency of release is less than 10^{-4} per year, but more than 10^{-6} per year. This frequency is not acceptable for events that have SL-1 level consequences, but is acceptable for events that have SL-2 level consequences. Therefore, the control strategy would need to provide enough mitigation to reduce the consequences of the release to the levels associated with a SL-2 event, as a minimum. The combined reliability of the preventive SSCs and the SSCs that provide mitigation needs to satisfy the target frequency for a SL-1 event. That is, the probability that the SSCs that provide mitigation will fail should be on the order of 10^{-2}, given the release.

~~SSCs in control strategies for SL-1 events shall satisfy the single failure criteria in the Implementing Standard for Defense in Depth.~~

For SL-2 events:

- ~~Meeting the target frequency will usually require a control strategy that incorporates diverse and independent SSCs that act to prevent and mitigate the event~~Application of the single failure criterion (imposing independency and/or diversity) may be required of prevention or mitigation controls to meet the target frequency for SL-2 events.
- The degree of mitigation required depends on the release frequency, that is, on the reliability of the preventive SSCs. For example, assume that the only viable preventive SSCs assure that the frequency of release is less than 10^{-2} per year, but more than 10^{-4} per year. This frequency is not acceptable for events that have SL-2 level consequences, but is acceptable for events that have SL-3 level consequences. Therefore, the preferred hazard control strategy would need to provide enough mitigation to reduce the consequences of the release to the levels associated with a SL-3 event, as a minimum. The combined reliability of the preventive SSCs and the SSCs that provide mitigation needs to satisfy the target frequency for a SL-2 event. That is, the probability that the SSCs that provide mitigation will fail should be on the order of 10^{-2}, given the release.
- ~~SSCs in control strategies for SL-2 events should satisfy the single failure criteria in the Implementing Standard for Defense in Depth.~~

For SL-3 and SL-4 events:

- The mitigation provided by the secondary confinement would be adequate to satisfy SRD Safety Criterion 2.0-1. It would also be adequate to satisfy SRD Safety Criteria 1.0-3 through 1.0-5. However, preventive features should be considered consistent with the defense in depth principle.
- A single preventive SSC may satisfy the frequency goal for SL-3 and SL-4 events.
- SSCs in control strategies for SL-3 and SL-4 events need not satisfy the single failure criteria in the Implementing Standard for Defense in Depth.

~~Notwithstanding the foregoing~~An exception to the above guidance on control strategy selection, administrative controls alone may be credited as the controls that protect facility workers, when appropriate. Timely evacuation from the vicinity of the hazard is considered to be an administrative control.

5.2 Approach for Direct Radiation Exposure Events

The general RPP-WTP design approach is to provide one passive physical barrier against exposure to direct radiation. For radiological materials that are contained with the process cells, the cell shield wall usually provides this barrier. For radiological material inventories located out of cells, container shielding usually serves as this barrier.

The accident severity levels defined in section 4.3.1 and the target frequencies identified in section 5.1 for radiological release events also apply to radiation exposure events.

When the preferred control strategy includes active systems and components (such as interlocks), then diversity and independence may be required to achieve the target frequency. Diversity and independence are generally not required for passive components to achieve the target frequency.

As was the case for radiological release events discussed in section 5.1, administrative controls alone may be credited as the controls that protect facility workers, when appropriate. Timely evacuation from the vicinity of the hazard is considered to be an administrative control.

5.3 Approach for Chemical Events

The potential consequences of hazardous chemicals shall also be assessed. The assessment shall consider both the inherent hazard of the chemical itself, and the potential for the chemical hazard to initiate or exacerbate a radiological hazard.

As many of the chemical hazards of the RPP-WTP are not unique to the facility, the selection of preferred hazard control strategies begins with the identificcation of what has been required and accepted as prevention and mitigation features for industrial plants with a similar chemical hazard. To implement this activity the ISM Team documents the types of prevention and mitigation features typically used at facilities with similar chemical hazards and comments on the appropriateness of the features for the RPP-WTP. Those that are appropriate for the RPP-WTP are identified as preferred hazard control strategies for preventing or mitigating the associated hazardous istuation for the RPP-WTP.

If the chemical hazard for the RPP-WTP poses a chemical risk that is unique to the RPP-WTP, additional (or augmented) accident prevention and/or mitigation features shall be considered. Some unique aspects of the RPP-WTP that would drive this consideration are:

1 The chemical hazard does not exist in many other facilities such that the database of prevention and mitigation features is limited.
2 The method of physically containing the hazardous chemical at the vitrification plant is different from normal industry practice.
3 The facility worker at the vitrification plant might work closer to the hazard.
4 The vitrification plant facility workers have less opportunity to isolate themselves from the chemical release (e.g., in industry practice the chemical is usually stored outside but for the RPP-WTP it is stored inside a building with a difficult egress).
5 The chemical hazard may lead to a hazardous situation that could adversely impact the ability of the operators to maintain the facility in a safe state.

6.0 Classification of Structures, Systems, and Components

Structures, systems, and components that serve as preferred hazard control strategies are classified as Important to Safety and further classified into subcategories of Important to Safety in accordance with SRD Safety Criterion 1.0-8. The quality levels assigned to this classification of SSCs and the attributes of these quality levels are provided in the Quality Assurance Manual (BNI 2001).

~~The design classification process used on the RPP-WTP Project provides a consistent, project-wide approach for the classification of the RPP-WTP SSCs based on their importance to controlling normal releases and accident prevention and mitigation. This approach ensures that SSCs are designed, constructed, fabricated, installed, tested, operated, and maintained to quality standards commensurate with the importance of the functions that need to be performed. As the facility moves to deactivation, and the safety functions change, the classification of SSCs can be revised as necessary.~~

~~The RPP-WTP project has established a design classification system to provide assurance to DOE that the defined safety functions of SSCs will perform as intended.~~

~~SSCs defined as Important to Safety for the RPP-WTP include the following:~~

~~1)SSCs needed to prevent or mitigate accidents that could exceed public or worker radiological and chemical exposure standards of Safety Criteria 2.0-1 and 2.0-2 and SSCs needed to prevent criticality. This set of SSCs includes both the front line and support systems needed to meet these exposure standards or to prevent criticality. This set of Important to Safety SSCs are designated as Safety Design Class, as defined by SRD Safety Criterion 1.0-8.~~

~~2)SSCs needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction. This set of Important to Safety SSCs are designated as Safety Design Significant, as defined by SRD Safety Criterion 1.0-8.~~

~~The processes for identifying the SSCs for each of the two groups of SSCs Important to Safety and the requirements assigned to each of the two groups are discussed below.~~

~~Safety Design Class SSCs typically are identified by the results of accident analyses that show the potential for exposure standards to be exceeded or prevent a criticality. However, additional items may also be designated Safety Design Class independent of a specific accident analysis. These are items that protect the facility worker from potentially serious events. Typically, these events are deemed to present a challenge to the facility worker severe enough that mitigation is prudent, without the need to perform a specific consequence analysis.~~

~~Safety Design Significant SSCs are identified in several ways including: (1) SSCs identified as significant contributors to safety by the analyses that confirm the facility accident risk goals are met (this is one way to identify SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction), (2) SSCs that are needed to ensure that standards for normal operation are not exceeded (e.g., bulk shield walls or radiation monitors), (3) SSCs selected based on the dictates of nuclear and chemical facility experience and prudent engineering practices, and (4) SSCs whose failure could prevent Safety Design Class SSCs from performing their safety function (e.g., Seismic II/I items).~~

~~When an SSC is designated as Safety Design Class it has the following attributes:~~

~~1)Quality Level 1 (QL-1) is applied to the SSC to provide added assurance that the SSCs can perform their specified safety function.~~

~~2)For an active system or component, the safety function is preserved by application of defense-in-depth such that failure of the system or component will not result in exceeding a public or worker accident exposure standard. For a mitigating feature, this means that, given that the accident has occurred, the consequence of the accident will not result in exceeding a public or worker exposure standard. For a preventative feature, this means that the failure of the system or component will not allow the accident to occur and progress such that a public or worker accident exposure standard is exceeded. If the hazard analysis shows that these requirements are necessary, this requirement may be achieved by designing the Safety Design Class system or component to withstand a single active failure or by designating two separate and independent systems or components as Safety Design Class.~~

~~3)The SSC is designed to withstand the effects of natural phenomena such that it can perform any safety functions required as a result of a natural phenomena event in accordance with Safety Criterion 4.1-3.~~

~~4)General design requirements are applied as identified in Chapter 4.0 of the SRD for Safety Design Class SSCs.~~

~~5)Specific design requirements based on the type of component are applied as invoked in SRD Chapter 4.0.~~

~~6)Other design requirements may be applied based on the specific safety function to be performed by the Safety Design Class SSC. This specific safety function is determined from the accident analysis that identified the need for prevention or mitigation by Safety Design Class SSCs.~~

~~7)Operational requirements (e.g., periodic testing and preventative maintenance) are applied to Safety Design Class SSCs through the application of Technical Safety Requirements.~~

~~When an SSC is classified as Safety Design Significant it is has the following attributes.~~

~~1)Quality Level 2 (QL-2) is applied to the SSC to provide added assurance that the SSCs can perform their specified safety function.~~

~~2)The SSC is designed to withstand the effects of natural phenomena such that it can perform its safety functions required as a result of a natural phenomena event in accordance with Safety Criterion 4.1-4.~~

~~3)General and specific design requirements are applied as identified in Chapter 4.0 of the SRD for Safety Design Significant SSCs.~~

~~4)Other design requirements again may be applied based on the specific safety function to be performed by the Safety Design Significant SSC.~~All text on this page has been deleted.

7.0 Identification of Standards

Identification of standards is an iterative activity. Initially, the set of standards and requirements is derived from a general understanding of the hazards and hazardous situations inherent in the work. As the design evolves, the hazard evaluation and the development of the preferred hazard control strategies justify tailoring the set of standards to better fit the hazards.

The identification of engineering/design, manufacture/fabrication, and construction standards is performed by an ~~integrated~~ ISM ~~t~~Team including work activity experts, hazard assessment experts, hazard control experts, as discussed in Sections 3.0 and 4.0, and standards experts. This ISM Team need not be the same team that performed the previous work identification and hazard evaluation activities. Identification of other standards (e.g., quality assurance, conduct of operations, etc.) will be performed by specially constituted teams formed by the PMT. The aim of this activity is to identify a tailored set of standards and requirements that will assure adequate safety when implemented.

The process management team shall provide additional technical resources as required to identify the standards.

Standards experts shall be drawn from the following RPP-WTP organizations:

- Staff of the Engineering Manager
- Technical staff of the Area Managers
- Technical staff of the ES&H Manager

The standards identified are evaluated and tailored for each control strategy based on compliance with applicable laws and regulations and conformance with the DOE-stipulated top level standards, plus the output of the preceding hazard evaluation and control strategy development steps. Typical considerations include the following:

- The severity level of the hazard
- The number of independent SSCs that comprise the preferred hazard control strategy
- The preferred hazard control strategy functions - recognizing that a specific control strategy may have multiple functions and serve to control multiple hazards
- The service (operating) environment (such as temperature and humidity)
- The applicable design basis events analysis
- The target reliability required of ~~for~~ the preferred hazard control strategy

The target frequencies described in Section 45.1 provide a basis for establishing target reliabilities for the SSCs that comprise the preferred hazard control strategy. The combined reliability of the preventive SSCs and the SSCs that provide mitigation must be consistent with the target frequency for the unmitigated event. The reliability of the preventive SSCs should be consistent with the release frequency used to determine the degree of mitigation provided.

Documentation of the standards and requirements identification process provides justification of the set selected and links each preferred hazard control strategy to its associated set of standards. The information generated during standards selection is retained in one or more databases form for each preferred hazard control strategy:

- Preferred hazard Ccontrol strategy
- Service environment
- Applicable design basis events
- Applicable standards
- Performance requirements
- Testing/calibration requirements
- In-service inspection requirements
- Maintenance requirements
- Quality level
- Standards justification

This information is structured so it can be linked to the preferred hazard control strategies in the hazard scheduleevaluation records. This provides a link from the hazards and hazardous situations through the preferred hazard control strategies to the standards. Not all of this information will be available early in the design. For example, it will not be possible to define maintenance and testing requirements until the design is mature.

~~The standards identified through this activity shall be reflected in the SRD.~~

As the standards are tailored, discrepancies with the current version of the SRD may arise. Such discrepancies shall be recorded. Formal changes to the SRD require approval from DOE.

8.0 Confirmation of Standards

Based on the recommendation of the PMT, the RPP-WTP Project Safety Committee (PSC) Chair requests the PSC to confirm the selected set of standards. The PSC defines a review approach, carries out the review, and documents the findings of the review. Comments by the PSC shall receive formal disposition by the Process Management Team.

9.0 Formal Documentation

Following confirmation by the PSC, the results of the standards selection process shall be documented in the ~~Safety Requirements Document (~~SRD~~)~~. The SRD shall incorporate documentation supporting these results by reference. The SRD shall identify and justify the set of requirements and standards selected to provide adequate protection of workers, the public, and the environment.

10.0 Recommendation

The recommended set of standards shall be certified in accordance with project implementing documents. When properly implemented, the set of standards:

1) provides adequate safety.
2) complies with applicable laws and regulations, and
3) conforms with the Top-Level Safety Standards and Principles.

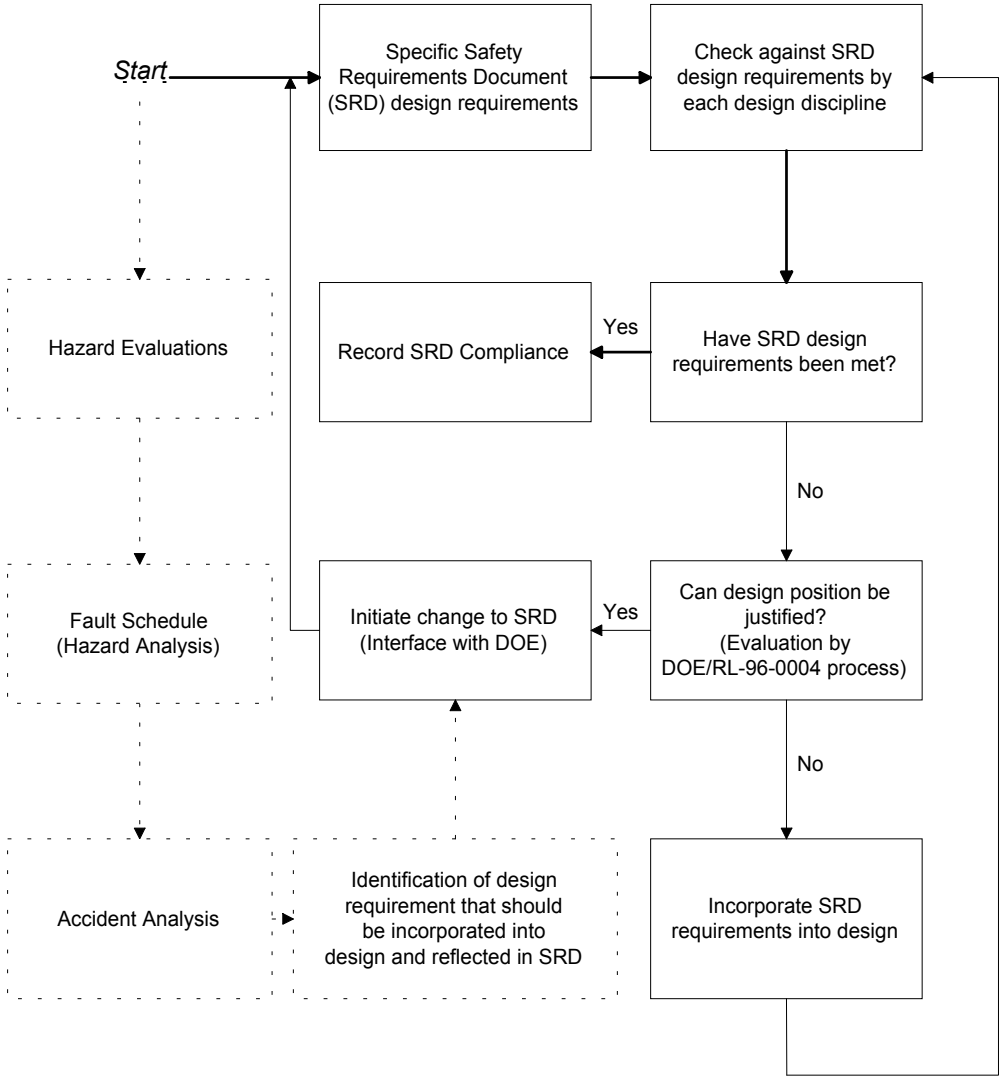
11.0 Maintenance of the SRD

Consistency of the SRD with current design information, hazards assessment, hazards control, and selected standards during the SRD development is ensured by participating with the personnel responsible for design and hazards analysis activities in the SRD development process as well as through reviews of the SRD, HAR, and design information. Additionally, for design-related criteria, a review of the Safety Criteria against facility design will be conducted to ensure the Safety Criteria are met by the design. Figure A-1 depicts this process.

Proposed changes to the SRD are evaluated for impact on safety and compliance with regulations and the authorization basis (including hazard and accident analysis). These changes are then reviewed and approved commensurate with the process applied to the original configureation, including regulatory approval prior to implementing changes that could be considered as decreasing the level of safety. The essential elements of DOE/RL-96-0004, *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for the RPP Waste Treatment Contractor*, as addressed in the original development of the SRD, are maintained, including the use of subject matter experts and the use of an equivalent level of review and approval of the proposed change.

After issuance of the construction approval, but prior to issuance of the SRD as part of the Operating Authorization Request package, the SRD will be controlled through the configuration management process. Additionally, DOE will be notified when the hazard analysis identifies a new situation affecting public safety or a significant revision occurs in a law or regulation that affects the design.

Figure A-1 SRD Compliance Process



12~~1~~.0 Definitions

Credible event: Any event with a frequency greater than 10^{-6} per year, including allowance for uncertainties.

Dependent Failures (Modarres 1993): In general, dependent failures are defined as events in which the probability of each failure is dependent upon the occurrence of other failures.

Important to Safety: Structures, systems, and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related, or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related, may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

Mitigated event: As used in this standard, a mitigated event involves the following sequence:

- An initiating event that could lead to a release from the primary confinement barrier
- Failure of all elements of the control strategy that would prevent the initiating event from developing into a release from the primary confinement barrier
- Mitigation of the consequences of the release as provided by the control strategy

Mitigated event frequency: The mitigated event frequency is the product of the corresponding release frequency ~~times~~ and the probability that the elements of the control strategy that mitigate the release will function given the release.

Release frequency: The release frequency is the product of the frequency of the initiating event ~~times~~ and the probability that all elements of the control strategy that would prevent the release fail, given the initiating event.

Reliability: The probability that an SSC will perform its safety function when required.

Unmitigated event: As used in this standard, an unmitigated event involves the following sequence:

- An initiating event that could lead to a release from the primary confinement barrier
- Failure of all elements of the control strategy that would prevent the initiating event from developing into a release from the primary confinement barrier
- Failure of all elements of the control strategy that would mitigate the consequences of the release

Unmitigated event frequency: The frequency of an unmitigated event is the corresponding release frequency times the probability that all elements of the control strategy that would mitigate the release fail, given the release.

13.0 References

AIChE, 1992, American Institute of Chemical Engineers (AIChE), *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples*, Center for Chemical Process Safety, New York, New York, USA, 1992.

BNI, 2001, *Quality Assurance Manual*, 24590-WTP-QAM-QA-01-001, Bechtel National, Inc., Richland, Washington, USA.

Modarres, 1993, *What Every Engineer Should Know about Reliability and Risk Analysis*, M Modarres, Marcel Dekker Inc., 1993, ISBN 0-8247-8958-X.

DOE/RL-96-0004, Revision 2, *Process of Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for the RPP Waste Treatment Plant Contractor.*

DOE/RL-96-0006, Revision 2, *Top-Level Radiological, Nuclear, and Process Safety Standards and Priniciples for the RPP Waste Treatment Plant Contractor.*

CONTENTS

1.0 Introduction B-1
2.0 Standards for the Implementation of Defense in Depth Sub-Principles B-1
2.1 Defense in Depth B-2
2.1.1 Implementing Standards B-2
2.1.2 Discussion B-2
2.2 Prevention B-4
2.2.1 Implementing Standards B-4
2.2.2 Discussion B-4
2.3 Control B-5
2.3.1 Implementing Standards B-5
2.3.2 Discussion B-6
2.4 Mitigation B-7
2.4.1 Implementing Standards B-7
2.4.2 Discussion B-7
2.5 Automatic Systems B-8
2.5.1 Implementing Standards B-8
2.5.2 Discussion B-8
2.6 Human Aspects B-9
2.6.1 Implementing Standards B-9
2.6.2 Discussion B-9
3.0 Determination of SSCs for the Implementation of Defense in Depth B-12
3.1 Radiological Release Events B-12
3.2 Direct Radiation Events B-14A
3.3 Chemical Release B-14B
4.0 Definitions B-15
5.0 References B-20
6.0 Tailoring of Consensus Standards Used in the Implementing Standard for Defense in Depth B-21
6.1 DOE O 420.1, Facility Safety (Ref. 5.2) B-21
6.2 Implementation Guide for Nonreactor Nuclear Safety Criteria and Explosives Safety Criteria (Ref. 5.3) B-21
6.3 ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions (Ref. 5.7) B-22
6.4 ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems (Ref. 5.8) B-22
6.5 IEEE STD 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (Ref. 5.9) B-23
6.6 IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11) B-24

6.7 IEEE STD 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (Ref. 5.12) B-25
6.8 ISA-S84.01-1996, Safety Instrumented Systems for the Process Industries (Ref. 5.13) B-25

1.0 Introduction

The purpose of this Implementing Standard is to consolidate the standards to be applied in the design, construction, and operation of the RPP-WTP with respect to defense in depth. This Implementing Standard also provides for tailoring of defense in depth as is appropriate to the nature and severity of the hazard and hazardous situations to which it is applied.

Section 2.0 identifies the subordinate standards used in the application of the six defense in depth sub-principles of DOE/RL-96-0006 (Ref. 5.4). These subordinate standards are derived, in part, from various available consensus standards. In cases where no relevant consensus standard exists for a given defense in depth sub-principle, this document provides the criteria to be implemented.

Section 3.0 discusses the approach to be used in implementing defense in depth with respect to determining an adequate combination of passive barriers and active SSCs that afford protection against a postulated initiating event.

Terms used in this Implementing Standard are defined in Section 4.0. These definitions are derived from DOE/RL-96-0006 and consensus standards, tailored to the work and hazards of the RPP-WTP.

2.0 Standards for the Implementation of Defense in Depth Sub-Principles

The Top Level Principles identify the following sub-principles that must be addressed in order to demonstrate compliance with the principle of defense in depth:

- Defense in depth
- Prevention
- Control
- Mitigation
- Automatic Systems
- Human Aspects

The following subsections contain the standards on application of the six sub-principles of defense in depth from DOE/RL-96-0006 (Ref. 5.4). These consensus standards will be tailored to remove obviously reactor-specific and other non-applicable criteria. In accordance with the DOE/RL-96-0004 (Ref 5.18) process, further tailoring will be performed as the design develops.

The following subsections contain excerpts and extracts from several consensus standards. Where necessary to avoid the implication of misquoting, differences in wording from the cited consensus standards are identified by presenting added words in italics and by inserting double-brackets where words have been removed. Citation of a portion of a given consensus standard shall not be read to infer that other portions of the standard not specifically cited are being invoked.

2.1 Defense in Depth

"To compensate for potential human and mechanical failures, a defense-in-depth strategy should be applied to the facility commensurate with the hazards such that assured safety is vested in multiple, independent safety provisions, not one of which is to be relied upon excessively to protect the public, the workers or the environment. This strategy should be applied to the design and operation of the facility." (DOE/RL-96-0006, Section 4.1.1.1)

2.1.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph
3. ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems (Ref. 5.8)
4. IEEE Std 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (Ref. 5.9)

2.1.2 Discussion

The RPP-WTP will be designed with the objective of providing multiple ~~*levels*~~ layers of protection to prevent or mitigate the unintended release of radioactive materials to the environment. Defense in depth will include: siting; minimization of material at risk; the use of conservative design margins and quality assurance; the use of successive physical barriers for protection against the release of radioactivity; the provision of multiple means to control critical safety functions (those basic safety functions needed to control the processes, maintain them in a safe state, and to confine and mitigate radioactivity associated with the potential for accidents with significant [ ] radiological impact *to the public, facility workers or collocated workers*); the use of equipment and administrative controls which restrict deviations from normal operations and provide for recovery from accidents to achieve a safe condition; means to monitor accident releases required for emergency responses; and the provision of emergency *preparedness* for minimizing the effects of an accident (Ref. 5.2).

The defense-in-depth concept is integrated into the RPP-WTP design process. The application of the defense-in-depth concept to the facility design helps identify potential safety features to be included in the facility design. Consideration will be given to prevent or mitigate accident consequences from contaminating the environment, even when direct public or facility or collocated worker safety is not an issue.

Defense in depth is a safety design concept or strategy that is applied at the beginning and will be maintained throughout the facility design process. This safety design strategy is based on the premise that no one layer ~~*level*~~ of protection is completely relied upon to ensure safe operation. This safety strategy provides multiple layers ~~*levels*~~ of protection to prevent or mitigate an unintended release of radioactive material to the environment.

Conceptually, there are three ~~levels~~ layers of defense in depth.

1. The first ~~level~~ layer of defense consists of a well-designed facility with process design to reduce source terms, reliable SSCs that are simple to operate and maintain and resistant to degradation, and personnel well trained in operations and maintenance and committed to a strong safety culture.
2. The second ~~level~~ layer recognizes that failures of systems and components and human failures cannot be entirely eliminated and that protective features (e.g., engineering design features and administrative controls) are required. These features are provided to ensure a return to normal operation or to bring the facility to a safe condition in the event of anticipated, but abnormal events. These features may provide automatic system response to such events or may be monitors that alert operators to the necessity of taking manual action. Such response to off-normal conditions can effectively halt the progression of events toward an accident.
3. The final ~~level~~ layer of defense consists of conservatively designed *important to* safety SSCs to prevent or mitigate the consequences of accidents that may be caused by errors, malfunctions, or events that occur both internal and external to the facility (Ref. 5.3).

Implementing Standards for the following elements of defense in depth described in the nonreactor safety Implementation Guide (IG) related to safety design and construction are addressed in the sections of this document that are referenced below.

IG Element	Discussed in Section
Siting	2.2.2
Material at risk	2.2.2
Conservative design	2.2.2
Quality assurance	2.6.2
Physical barriers	2.4.2
Critical safety functions	2.3.2
Equipment and administrative controls	2.3.2 and 2.6.1
Emergency features	2.5.2

When ~~active SSCs are required to achieve defense in depth, RPP-WTP will apply~~ the single failure criterion is implemented, it is done in accordance with ANSI/ANS-58.9 (Ref. 5.8) for fluid systems and IEEE Std 379 (Ref. 5.9) for electrical and instrumentation and control systems~~, as discussed below~~. As indicated in Table 1, application of the single failure criterion is required of prevention and mitigation controls credited for meeting exposure standards for radiological release events of Severity Level 1. It may also be required of SL-2 events to meet the target frequency.

The application of the single failure criterion begins with the identification of an initiating event. Initiating events are identified in the normal course of applying integrated safety management in accordance with DOE/RL-96-0004, as described in the RPP-WTP Implementing Standard for Safety Standards and Requirements Identification (i.e., SRD Vol. II, Appendix A). In evaluating the defense in depth of the RPP-WTP, single failures must be postulated in addition to the initiating event (that is the initiating event is not the single failure) (Ref. 5.8). For fluid systems, during the short term, the single failure considered may be limited to an active failure. During the long term, assuming no prior failure during the short term, the limiting single failure considered can be either active or passive. Examples of passive failures are valve packing and pump seal leakage.

Tailoring of the application of the single failure criterion to the work and associated hazards is discussed in Section 3.0.

2.2 Prevention

"Principal emphasis should be placed on the primary means of achieving safety, which is the prevention of accidents, particularly any that could cause an unacceptable release." (DOE/RL-96-0006, Section 4.1.1.2)

2.2.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph

2.2.2 Discussion

The provision of hazard elimination and protection shall be optimized by measures such as the choice of siting, proven conservative design and construction, a robust start-up testing program, operating requirements (i.e., clear definition of normal and abnormal operating conditions and maintenance activities).

Siting. The RPP-WTP site location will reduce the need to provide design measures to alleviate potentially hazardous conditions or to protect surrounding populations (for example, consideration of ground instability, river flooding, and hazards due to nearby industrial installations or activities) (Ref. 5.3).

Material at Risk. The RPP-WTP and its process design and administrative controls will minimize and control inventories of radioactive materials and their forms (Ref. 5.3).

Conservative Design. The RPP-WTP design will include conservative margins that allow flexibility of operations and maximize the time before requiring corrective actions. These margins will also take into consideration the potential degradation of elements and operational errors (Ref. 5.3).

The site for the facility has been established by DOE. Aspects of siting that remain for consideration include:

1 the risk that the site presents to the facility in terms of natural phenomena and nearby industry and transportation, and

2 the risk that the facility presents to the nearby environment, collocated workers, and the public.

Defense in depth for protection against NPH events is achieved by:

1 the selection of NPH loadings of SRD Safety Criteria 4.1-3 and 4.1-4 that have a low frequency of occurrence in the lifetime of the facility with the most severe events having the lowest frequency of occurrence, and

2 the selection of design, fabriaction, and construction standards that provide a significant margin to failure should the NPH loading be experienced.

Protection against accidents at nearby industry and transportation locations is addressed by conservative analyses of radiological and chemical release, overpressure, and physical impact events related to these facilities.

The vitrification project does not have control over the environment or population (colocated worker and public) outside the controlled area. However, all of the sub-principles of defense in depth discussed in Section 2.0 provide for protection of the environment, collocated woker, and public against the unconctrolled release of chemical and radiological materials from the facility.

The design shall address all identified hazards and hazardous situations and pursue methods for their prevention. The preferred means of prevention is to eliminate or reduce the severity of the hazard itself. According to the Implementation Guide on nonreactor facility safety, one objective of prevention as an element of defense in depth is to apply facility and process design and administrative controls to minimize and control inventories of radioactive materials and their forms (that is, minimize the material at risk) (Ref. 5.3).

Elimination or reduction of the hazard can be achieved by substituting less hazardous materials in processing, limiting the inventory of the material, etc. The design process must provide evidence through documentation that this option was considered and implemented to the maximum extent practicable. Where the hazard itself cannot be eliminated or reduced, controls shall be provided to reduce the likelihood of the hazard manifesting itself into an accident. The criterion for acceptability is discussed in Section 3.0. Where hazard elimination is not practicable, passive features are to be employed, since they are simple and have a high degree of reliability. Where this is not practicable, active protection will be proposed that has a degree of reliability and confidence commensurate with the potential hazard severity.

Conservatism in design is achieved in part by requiring a significant margin between the design limit and the ultimate failure point of a SSC. Conservatism in design is also accomplished by giving preference to passive over active components, material selection, keeping systems as simple in their operation and maintenance as possible, including provisions for corrosion and erosion, prevention, and the mitigation of mis-operation of systems and components (e.g., by the use of interlocks), and redundancy and diversity to accommodate system and component failures.

~~To illustrate the differences between hazard elimination and the provision of passive or active protection, consider the need for a cask lift using a crane. Elimination of the hazardous situation (inherent safety) is removal of the potential for raising a cask above its safe drop height by ensuring that the building dimensions physically prevent a lift above that height at all points of travel. If this were not practical, the provision of a physical stop would be passive protection to prevent a lift above the safe drop height. Active protection systems would include limit switches and braking systems. Procedures and operator training would ensure that the crane is handled and operated in a way that maximizes safety (e.g., check security of load, minimum lift height to confirm security, no challenge to engineered systems, and exclusion of personnel from load lifting area).~~

2.3 Control

"Normal operation, including anticipated operational occurrences, maintenance and testing, should be controlled so that facility and system variables remain within their operating ranges and the frequency of demands placed on structures, systems and components important to safety is small." (DOE/RL-96-0006, Section 4.1.1.3)

2.3.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph
3. IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11)
4. ISA-S84.01-1996, Application of Safety Instrumented Systems for the Process Industries (Ref. 5.13)

2.4 Mitigation

"The facility should be designed to retain the radioactive material through a conservatively designed confinement system for the entire range of events considered in the design basis. The confinement system should protect the workplace and the environment." (DOE/RL-96-0006, Section 4.1.1.4)

2.4.1 Implementing Standards

1. DOE O 420.1 (Ref. 5.2), Section 4.1.1.2, first three paragraphs only
2. Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria (Ref. 5.3), Section 2.3, except last paragraph
3. Safety Requirements Document

2.4.2 Discussion

~~The purpose of m~~Mitigation is implemented to ensure reduction of consequences from potential hazards and hazardous situations such that the applicable exposure standards are satisfied. One method of achieving this element of defense in depth is to ensure that suitable confinement of radioactive and hazardous material is maintained throughout normal operation and credible accident conditions. Confinement will be achieved by physical barriers and by other SSCs that either assure integrity of the physical barriers or minimize the quantity and characteristics of any hazardous material potentially releasable.

DOE Order 420.1, Chg 2, requires:

> "All nuclear facilities with uncontained radioactive materials (as opposed to material contained within drums, grout and vitrified materials) shall have means to confine them. Such confinement will act to minimize the spread of radioactive materials and the release of radioactive materials in facility effluents during normal operations and potential accidents. For a specific nuclear facility, the number and arrangement of confinement barriers and their required characteristics shall be determined on a case-by-case basis. Factors that shall be considered in confinement system design shall include type, quantity, form, and conditions for dispersing the material. Engineering evaluations, trade-offs, and experience shall be used to develop practical designs that achieve confinement system objectives. The adequacy of confinement systems to effectively perform the required functions shall be documented and accepted through the Safety Analysis Report." (Ref. 5.2)

The DOE nonreactor facility safety Implementation Guide defines confinement barriers to include primary confinement and secondary confinement. "Primary confinement provides confinement of hazardous material to the vicinity of its processing -- typically by means of piping, tanks, glove boxes, encapsulating material, etc., along with any offgas systems that control effluent from the primary confinement. As such, primary confinement addresses the preventive sub-principle of defense in depth, as well as mitigation. Secondary confinement consists of a cell or enclosure surrounding the process material or equipment along with any associated ventilation exhaust systems from the enclosed area." [ ] (Ref. 5.3)

The RPP-WTP will provide physical barriers to confine radioactive material and thereby prevent uncontrolled releases. In general, multiple physical barriers - i.e., primary and secondary confinement - will be provided, especially for the most severe hazards and hazardous situations. Although RPP-WTP buildings will afford a tertiary confinement, as defined in the Implementation Guide, the RPP-WTP accident analysis will not take credit for holdup of radioactive materials by the buildings. The provision of multiple physical barriers will be tailored to the work and associated hazards, as discussed in Section 3.0.

The DOE nonreactor facility Implementation Guide (IG) suggests several industry consensus codes and standards for the design and construction of the SSCs comprising confinement, as follows: structures - IG subsection 5.2.1, ventilation systems - subsection 5.2.2.1, and process equipment - subsection 5.2.2.2. The specific standards for SSCs that implement mitigation with respect to SSCs comprising confinement are contained in the following Safety Criteria from the Safety Requirements Document:

- Structures - SC 4.1-2
- Ventilation systems - SC 4.4-6 through 4.4-8
- Process equipment - SC 4.2-1 through 4.2-3

2.5 Automatic Systems

"Automatic systems should be provided that would place and maintain the facility in a safe state and limit the potential spread of radioactive materials when operating conditions exceed predetermined safety setpoints." (DOE/RL-96-0006, Section 4.1.1.5)

2.5.1 Implementing Standards

1. IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11)
2. ISA-S84.01-1996, Application of Safety Instrumented Systems for the Process Industries (Ref. 5.13)
3. ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions (Ref. 5.7)

2.5.2 Discussion

Automatic systems shall be provided to prevent the facility from entering into or remaining within an unsafe regime that may lead to the potential for radioactive or hazardous material release to facility and collocated workers, the public, or the environment, except as discussed below. The definition of the boundaries between safe and unsafe regimes will be determined as a result of detailed facility design, start-up, and testing activities. This will allow the derivation of the predetermined setpoints for safe facility operations. Automatic systems will be part of the overall suite of SSCs provided as part of the hazard control strategy. The determination of the need for automatic systems will be assessed as part of the determination of the overall hazards control strategy.

IEEE Std 1023-1988 was developed specifically for nuclear power generating stations. Therefore, this subordinate standard will be tailored to the work and hazards of the RPP-WTP as follows. The formal HFE process described in subsection 6.1.1 of IEEE Std 1023-1988 will be applied to the evaluation of hazards whose consequences fall into the two highest severity levels - SL-1 and SL-2 (see in SRD Volume II, Appendix A, section 4.3.1), with the following clarification:

> The project does not plan on constructing a separate plant simulator or physical mockup. The RPP-WTP distributed control system (DCS) - including the main control room panels -- is a programmable computer system. The project envisions having the DCS built, delivered to the site and proof-tested with the aid of the facility operators well in advance of plant startup. Therefore, a dynamic simulation capability for personnel training will be provided for SSCs with significant human interfaces that involve complex and interactive processes (Ref. IEEE Std 1023-1988 §§ 6.1.1.12 and 6.1.1.18).

Although the structured HFE program outlined in subsection 6.1.1 of IEEE Std 1023-1988 will not be implemented for SL-3 and SL-4 events, the general HFE elements will be considered for all ITS SSCs, as committed above.

Similarly, formal consideration of the HFE techniques and methodologies recommended in Section 5 of IEEE Std 1023-1988 will be undertaken for hazards of severity levels SL-1 and SL-2. Certain of these techniques and methodologies may be utilized in the evaluation of SL-3 and SL-4 events in the context of the normal design and hazard assessment and control effort, as part of the integrated safety management process.

Quality Assurance Program

The Safety Requirements Document Safety Criteriaon 1.0-10 and Section 7.3 require the RPP-WTP contractor to establish and implement a quality assurance program compliant with 10 CFR 830.120. This program is being implemented in accordance with the Quality Assurance Manual (QAM) (24590-WTP-QAM-QA-01-001).

The QAM applies specifically to work performed on or for the RPP-WTP. The QAM is in conformance with 10 CFR 830.120 (Ref. 5.1) and with the top-level principles stated in DOE/RL-96-0006 (Ref. 5.4).

Administrative Controls

Administrative controls include features to control process variables to values within normal and safe conditions, to monitor equipment status, to alert operating personnel of an approach toward conservative process limits, to allow timely detection of failure or malfunction of critical equipment, and to allow for the imposition of administrative controls assumed in the hazard analysis, and/or accident analysis (Ref. 5.3).

The primary means of implementing defense in depth is through the provision of multiple physical barriers that maintain confinement. The output of the design process, through which hazards and hazardous situations are identified, control strategies implemented and standards defined will be a set of SSCs that ~~achieve~~ contribute to defense in depth. SSCs so identified will always be backed up by administrative controls such as procedures. Administrative controls that afford a measure of defense in depth will be developed prior to facility operations. For the purpose of protecting the public and collocated worker, administrative controls alone shall not be relied on for the implementation of defense in depth. Administrative controls alone may be credited as the controls that protect facility workers, when appropriate. In such cases, defense in depth is provided through other human aspects, such as worker qualification and training.

Internal Safety Reviews

The Safety Requirements Document, Safety Criterion 7.1-3, requires that the RPP-WTP contractor establish a safety framework and specifies requirements for the Internal Safety Oversight program consistent with Top-Level Principle 4.4.1, "Safety Review Organization". BNI has established a RPP-WTP Project Safety Committee (PSC) to provide an independent, interdisciplinary evaluation of matters related to nuclear, radiological, and process safety.

Operating Limits (Technical Safety Requirements)

The Safety Requirements Document, Safety Criterion 9.2-1, commits the RPP-WTP contractor to prepare, submit for approval, and operate the facility in accordance with Technical Safety Requirements (TSRs). SCs 9.2-2 through 9.2-6 provide the safety criteria for the bases and contents, updating, submission for regulatory approval, and maintenance of TSRs.

As part of hazard evaluation, the role of the operator in the development of a potential hazard will be identified and reliability assessed. Human factors specialists in the multidisciplinary team will support this evaluation. The results of the assessment will be incorporated into administrative controls such as operating procedures and TSRs.

Worker Qualification and Training

The Safety Requirements Document, Section 7.2, commits the RPP-WTP contractor to establish and implement a training program. Consistent with Top-Level Principles 4.3.4.1, "Personnel Training", 4.3.4.2, "Training Programs", and 5.2.4, "Process Safety - Training," SRD Volume II, Section 7 requires that the program address:

- continual training - SC 7.2-1, 7.2-3, 7.3-3
- qualification of personnel - SC 7.3-3
- records of training status - SC 7.2-4
- establishment of written procedures/instructions - SC 7.2-2, 7.2-5

Establishment of a Safety/Quality Program

The Safety Requirements Document, Safety Criteria 1.0-1, requires the use of a comprehensive safety management program consistent with Top-Level Principle 5.1.1, "Process Safety Management", and 5.1.2, "Process Safety Objective". Safety Criterion 7.1-3 requires a safety framework be established to implement this Program consistent with Top-Level Principle 4.1.4.1, "Safety/Quality Culture".

Establishment of a Quality Program is discussed above under the heading, "Quality Assurance Program".

3.0 Determination of SSCs for the Implementation of Defense in Depth

The standards for prevention, control, and human aspects in Sections 2.2, 2.3, and 2.6 are primarily concerned with defense in depth sub-principles that minimize the potential of hazard initiation. In evaluating accidents that are postulated to occur despite implementation of preventive, control and human aspects, the sub-principles of mitigation and automatic systems must be considered.

The Implementing Standard for Safety Standards and Requirements Identification, SRD Volume II, Appendix A, describes the process by which hazards and hazardous situations are identified and evaluated to determine hazard control strategies. Use of this SRD Appendix A with this Appendix B Implementing Standard ensures that the defense in depth sub-principles are accounted for in the process of determining hazard control strategies. That process will identify SSCs that ~~perform~~ contribute to defense in depth as part of their safety function. The administrative controls that back up these SSCs will be developed prior to the introduction of hazardous materials into the facility.

In addition to the identification of defense in depth SSCs through implementation of SRD Volume II, Appendices A and B, the requirement to satisfy the accident risk goals of SRD Safety Criteria 1.0-3 and 1.0-5 may require the identification of additional accident prevention or mitigation SSCs.

3.1 Radiological Release Events

Table 1 is the standard for implementing defense in depth by SSCs as part of the preferred hazard control strategy; it defines the minimum number of SSCs and associated engineering requirements for the control of radiological release hazards of a particular severity.

Table 1 will be used in conjunction with the guidance in Section 2.0 to ensure that the preferred hazard control solution addresses the strategies that protect the public and collocated workers from the uncontrolled release of radiological materials; such SSCs will always be backed up by the human aspects of defense in depth discussed in Section 2.6.

The table lists the number and attributes of the physical barriers, as well as the application of the single failure criterion to SSCs that are required to adequately implement defense in depth for a given preferred hazard control strategy. Confirmation of the adequacy of implementation is achieved by meeting the numerical guidance stated in the third column. Consistent with the defense in depth sub-principles in Section 2.0, the preferred hazard control strategy should emphasize passive SSCs over active SSCs.

Hazard severities and target frequencies are ~~the means to achieve adequate~~a tailored approach that contributes to achieving defense in depth in accordance with the tailored approach mandated by RL/REG 98-17, "Regulatory Unit Position on Tailoring for Safety."

1st Column - SL (Severity Level)

Determination of hazard severity level is based on an assessment of unmitigated consequences as discussed in SRD Volume II, Appendix A, Section 4.3.1. Severity levels are defined as SL-1 to SL-4, with SL-1 having the highest consequences.

2nd Column - Control Options for Implementation of Defense in Depth

A graded approach is reflected in the configuration requirements against each hazard severity level. The requirements are more stringent for defense in depth implementation for hazards of greater severity than for those of lesser severity.

Implementation of defense in depth requires that the single failure criterion be applied in a tailored fashion. For SL-1, application of the single failure criterion is mandatory. The single failure criterion is applied to the set of two or more barriers credited for meeting the exposure standards and target frequency. For SL-2, the single failure criterion ~~shall~~ may be considered; that is, an objective assessment ~~must~~ may be performed to determine the extent to which the single failure criterion will be incorporated into or be satisfied by design. This assessment includes consideration of the need to provide for protection against single failures to achieve the required target frequency. The results and basis of this assessment shall be documented. Such documentation shall be retrievable and can be in the form of engineering studies, meeting minutes, reports, internal memoranda, etc. The single failure criterion is discussed in Section 2.1.

In addition to the single failure criteria in Table 1, diversity may also be implemented in the control strategy where hazards assessment reveals a common mode failure concern (see the Implementing Standard for Safety Standards and Requirements Identification, SRD Vol. II, Appendix A).

Implementation of defense in depth also requires that the provision of physical barriers be applied in a tailored fashion as noted in Table 1. ~~In Table 1, provision of physical barriers refers to those that provide confinement against the release of hazardous materials, as opposed to barriers that protect against direct radiation.~~ For SL-1 and SL-2, two or more independent physical barriers are required. For SL-3, at least one physical barrier shall be provided, and two or more independent physical barriers shall be considered; that is, an objective assessment must be performed to determine the extent to which physical barriers will be incorporated by the design. The results and basis of this assessment shall be documented. Such documentation shall be retrievable and can be in the form of engineering studies, meeting minutes, reports, internal memoranda, etc~~. For SL-4, physical design features and/or administrative controls per 10CFR 835.1001 shall be provided~~.

The graded approach is also reflected in the degree of confidence required commensurate with the hazard severity. The confidence is based on the standards and other attributes applicable to the particular control strategy. The Implementing Standard for Safety Standards and Requirements Identification describes selection of standards and other attributes applicable to control strategies.

3rd Column - Target Frequency (yr^{-1})

This column lists the target frequencies for each hazard severity level. The hazard severity level is a measure of the consequence from an unmitigated event - that is, an event in which both SSCs that prevent the accident and SSCs that mitigate the accident fail. After the preferred hazard control strategy has been identified, the event frequency - i.e., the product of the frequency of the initiating event and the probability that the control strategy will fail given the initiating event - will be conservatively estimated. (No credit is taken for administrative controls in calculating the initiating event frequency.) Verifying that the event frequency is less than the target frequency will provide confirmation that the chosen control strategy includes sufficient SSCs to adequately implement this aspect of defense in depth (i.e., the selection of hazard control strategies) in a graded approach.

The demonstration of having met the target frequencies may be based on either numerical analysis or engineering judgment. When appropriate, administrative controls alone may be credited as the controls that protect facility workers. The hazard assessment and control team shall assess the confidence in the frequency so determined, applying greater conservatism where engineering judgment is employed.

Table 1. Implementation of Defense in Depth by SSCs for Radiological Release.

Severity Level (SL)	Control Options for Implementation of Defense in Depth	Target Frequency (yr^{-1})
SL-1	Two or more independent physical barriers. The single failure criterion shall be applied to the set of two or more barriers credited for meeting exposure standards and target frequency.	$< 10^{-6}$
SL-2	Two or more independent physical barriers. ~~The single failure criterion shall be considered~~Application of the single failure criterion may be required of prevention or mitigation controls to meet the target frequency.	$< 10^{-4}$
SL-3	At least one physical barrier shall be provided. Two or more independent physical barriers shall be considered.	$< 10^{-2}$
SL-4	Physical design features and/or administrative controls per 10 CFR 835.1001	$< 10^{-1}$
Administrative controls alone may be credited as the controls that protect facility workers, when appropriate. Timely evacuation from the vicinity of the hazard is considered to be an administrative control. Physical barriers are not required for those events that are prevented (i.e., the product of the initiating event frequency and the conditional failure probability of the prevention system(s) is $< 10^{-6}$/yr).		

3.2 Direct Radiation Events

Because of the distances involved, direct radiation is primarily a hazard to the facility worker as opposed to the collocated worker or the public. Direct radiation hazards usually involve:

1 accidents that result in a release of radiological material or loss of shielding such that time, distance, and/or shielding are adversely affected, or

2 inadvertent facility worker entry into an area with a high radiation field.

Mitigation of the first type (accidents involving a radiological release) is usually accomplished by the use of passive shield walls. Prevention of the second type (entry into a high radiation field) usually involves the use of engineered and administrative controls to prevent the entry into areas with a high radiation field.

Implementation of defense in depth by SSC for direct radiation events begins in a manner similar to that used for radiological releases; that is, by the the assignment of severity levels based upon unmitigated consequences.

Table 2 is the standard for implementing defense in depth by SSCs as part of the preferred hazard control strategy related to the prevention and mitigation of direct radiation accidents. The basic description of the first and third columns is the same as that provided in section 3.1 for accidents involving radiological releases.

Table 2. Implementation of Defense in Depth by SSC for Direct Radiation Hazards.

Severity Level (SL)	Control Options for Implementation of Defense in Depth	Target Frequency (yr^{-1})
SL-1	One passive physical barrier that is not challenged by the event; two independent barriers if the first barrier might be challenged by the event or is not totally passive.	$< 10^{-6}$
SL-2	One passive physical barrier that is not challenged by the event; two independent barriers if the first barrier might be challenged by the event or is not totally passive.	$< 10^{-4}$
SL-3	One physical barrier.	$< 10^{-2}$
SL-4	One physical barrier or administrative controls.	$< 10^{-1}$
Administrative controls alone may be credited as the controls that protect facility workers, when appropriate. Timely evacuation from the vicinity of the hazard is considered to be an administrative control. Physical barriers are not required for those events that are prevented (i.e., the product of the initiating event frequency and the conditional failure probability of the prevention system(s) is $< 10^{-6}$/yr).		

Where passive barriers are provided and the barriers would not be challenged by the event (e.g., insignificant pressurization of a cell relative to its inherent strength) it is not necessary to estimate probability of failure to determine the unmitigated event frequency. Where active components or systems are included in the control option (e.g., an interlock on a shield door), the unmitigated event frequency must be calculated for comparison with the target frequency. The unmitigated event frequency must also be calculated for passive SSCs that might be challenged by the event.

3.3 Chemical Release

The potential consequences of hazardous chemicals shall also be assessed. The assessment shall consider both the inherent hazard of the chemical itself, and the potential for the chemical hazard to initiate or exacerbate a radiological hazard.

As many of the chemical hazards of the vitrification facility are not unique to the facility, the selection of preferred hazard control strategies includes identification of what has been required and accepted as engineered prevention and mitigation features for industrial plants with a similar chemical hazard. The chemical hazard for the vitrification facility is also reviewed to determine if it has a chemical risk that is somewhat unique to the facility. When such a case is identified, consideration is given to additional (or augmented) accident prevention and/or mitigation engineered features.

Additional detail on the selection of preferred hazard control strategies for chemical hazards and hazardous situations is provided in the SRD Volume II, Appendix A, "Implementing Standard for Safety Standards and Requirements Identification".

4.0 Definitions

Definitions of the following terms were obtained from the referenced consensus standards. Minor wording differences among multiple references are ignored. In some cases, the definition of a term given in the referenced consensus standard has been tailored to the relative risks of the RPP-WTP and its anticipated associated hazards. Other wording differences in the definitions below from the cited consensus standards have been made to preserve consistency with terminology in other RPP-WTP safety documentation. Such differences are identified by presenting added words in Italics and by inserting double-brackets where words have been removed. Citation of a definition from a given consensus standard shall not be read to infer that other portions of the standard not specifically cited are being invoked.

Active component [SSC]. A component in which mechanical movement must occur to accomplish the [ ] safety function of the component (Ref. 5.5, 5.6)

Active failure. A malfunction, excluding passive failures, of a component that relies on mechanical movement to complete its intended [ ] safety function upon demand

Examples of active failures include the failure of a valve or check valve to move to its correct position, or the failure of a pump, fan, or diesel generator to start.

Spurious action of a powered component originating within its actuation or control system shall be regarded as an active failure unless the specific design features or operating restrictions preclude such spurious action. An example is the unintended energization of a powered valve to open or close (Ref. 5.5, 5.6, 5.8).

Administrative controls. Provisions relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure safe operation of the facility.

Barrier. A control that has the function of maintaining confinement or shielding, and that is preventing or mitigating either: (1) the release of radioactive or hazardous material to the facility or co-located worker, public, or the environment; or (2) the exposure at the facility or co-located worker or the public to sources of direct radiation. This control can be an SSC that provides a physical barrier (e.g. vessel, shielding, and filtration) or an administrative control (e.g., training and procedures), which supplements the physical barriers.

Common cause failure. Dependent failures that are caused by a condition external to a system or set of components that make system or multiple component failures more probable than multiple independent failures (Ref. 5.4).

Common mode failure. Dependent failures caused by susceptibilities inherent in certain systems or components that make their failures more probable than multiple independent failures due to those components having the same design or design conditions that would result in the same level of degradation (Ref. 5.4).

Confinement. Physical barrier that prevents or mitigates the release of radioactive or hazardous material to the worker, public or the environment. The DOE nonreactor facility safety Implementation Guide identifies three kinds of confinement barriers - primary confinement, secondary confinement, and tertiary confinement (Ref. 5.3).

Control strategy. A set of generally-described provisions (barriers, dilution/dispersal, physical limitations on material quantities, administrative material controls, confinement, ventilation of flammable gas, etc.) and/or approaches (defense in depth, use of passive features, prevention, mitigation, etc.) which are intended to assure adequate control of a specific hazard and associated accidents in the context of the work (Ref. 5.4).

Defense in depth. The fundamental principle underlying the safety technology of the facility centered on several levels of protection including successive barriers preventing the release of radioactive materials to the workplace or the environment. Human aspects of defense in depth are considered to protect the integrity of the barriers, such as quality assurance, administrative controls, safety reviews, operating limits, personnel qualifications and training and safety program. Design provisions including both those for normal facility systems and those for systems important to safety help to: 1) prevent undue challenges to the integrity of the physical barriers; 2) prevent failure of a barrier if challenged; 3) where it exists, prevent consequential damage to multiple barriers in series; and 4) mitigate the consequences of accidents. Defense in depth helps to assure that two basic safety functions (controlling the process flow and confining the radioactive material) are preserved and that radioactive materials do not reach the worker, public or the environment (Ref. 5.4).

Dependent Failures (Modarres 1993). In general, dependent failures are defined as events in which the probability of each failure is dependent upon the occurrence of other failures.

Design Basis Events. Postulated events providing bounding conditions for establishing the performance requirements of structures, systems and components that are necessary to: 1) ensure the integrity of the safety boundaries protecting the worker; 2) place and maintain the facility in a safe state indefinitely; or 3) prevent or mitigate the event consequences so that the radiological exposures to the general public or the workers would not exceed appropriate limits. The Design Basis Events also establish the performance requirements of the structures, systems, and components whose failure under Design Basis Event conditions could adversely affect any of the above functions (Ref. 5.4).

Detectable failures. [The following definition is considered to be specific to electrical, instrumentation and control systems.]

> Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication (Ref. 5.9).

Diversity. Use of different technologies, equipment, or design methods to perform a common function with the intent to minimize common cause failures (Ref. 5.13).

Engineered feature. A structure, system or component that contributes to the safe operation of the facility (Ref. 5.14).

Event. A condition that deviates from normal operation, i.e., an initiating occurrence plus single failure or coincident occurrence combination (Ref. 5.5, 5.6).

5.0 References

5.1 10 CFR 830.120, "Quality Assurance Requirements".

5.2 DOE O 420.1, *Facility Safety*, Chg 2, 10/24/96.

5.3 *Implementation Guide for Nonreactor Nuclear Safety Criteria and Explosives Safety Criteria*, Revision G (Draft), September 1995.

5.4 DOE/RL-96-0006, Revision ~~1~~2, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for ~~TWRS Privatization~~the RPP Waste Treatment Plant Contractor~~s~~.*

5.5 ANSI/ANS-51.1-1983, *Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants. American Nuclear Society*.

5.6 ANSI/ANS-52.1-1983, *Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants. American Nuclear Society*.

5.7 ANSI/ANS-58.8-1994, *Time Response Design Criteria for Safety-Related Operator Actions. American Nuclear Society*.

5.8 ANSI/ANS-58.9-1981, *Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems. American Nuclear Society*.

5.9 IEEE Std 379-1994, *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*. IEEE Power Engineering Society.

5.10 IEEE Std 384-1992, *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits. IEEE Power Engineering Society*.

5.11 IEEE Std 603-1991, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. IEEE Power Engineering Society*.

5.12 IEEE Std 1023-1988, *IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations*.

5.13 ISA-S84.01-1996, *Application of Safety Instrumented Systems for the Process Industries. Instrument Society of America*.

5.14 *Integrated Safety Management Plan*. ~~BNFL-5193-ISP-01, Revision 3~~24590-WTP-ISMP-ESH-01-001. ~~BNFL Inc., July 7, 1998~~Bechtel National, Inc., Richland, WA.

5.15 *Guidelines for Hazards Evaluation Procedures, Second Edition with Worked Examples*. Center for Process Chemical Safety, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 1992.

5.16 DOE O 6430.1A, General Design Criteria, 6 April 1989.

5.17 Modarres, 1993, *What Every Engineer Should Know about Reliability and Risk Analysis*, M Modarres, Marcel Dekker Inc., 1993, ISBN 0-8247-8958-X.

5.18 DOE/RL-96-0004, Revision 2, *Process of Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for the RPP Waste Treatment Plant Contractor*.

2.0 Exposure Standards for Facility and Collocated Workers

The four "To be derived" cells in DOE Table 1 have been completed by imposing a radiological exposure standard not to exceed 25 rem/event to the RPP-WTP facility workers or to collocated workers for either unlikely or extremely unlikely events.

The 25 rem/event exposure standard for both the facility and collocated workers for unlikely and extremely unlikely events corresponds to the once-in-a-lifetime accident or emergency exposure for radiation workers which, by recommendation of the National Committee on Radiation Protection (NCRP 1963), may be disregarded in the determination of their radiation exposure status. In addition, an exposure of 25 rem/event corresponds to a conditional probability of fatality of about 2×10^{-2}. For unlikely events (defined in Table 2-1 as having a maximum occurrence frequency of 10^{-2}/yr), this equates to a maximum increase in worker lifetime risk of premature death of only 2×10^{-4}, which is considerably less than the average accidental death risk for workers in some of the safest industries (i.e., retail and wholesale trade, manufacturing, and service [EPA 1991]).

Compliance with the 25 rem/event standard is established using qualitative methods supported, where necessary, by numerical analysis that may include the development of event trees and fault trees and/or the performance of consequence analyses. From this process, preventative and mitigative engineered and administrative controls are identified.

Use of qualitative methods is consistent with the American Institute of Chemical Engineers (AIChE) guidelines (AIChE 1992), U.S. Nuclear Regulatory Commission (NRC) guidance for the performance of integrated safety analysis for 10 *Code of Federal Regulations* (CFR) 70 special nuclear material licensees (NRC 1995a), as well as DOE-STD-3009 (DOE 1994) and DOE G 420.1-X (DOE 1995). Both DOE documents state the following:

> "Estimates of worker consequences for the purpose of a safety-significant SSC designation are not intended to require detailed analytical modeling. Considerations should be based on engineering judgement of possible effects and the potential added value of safety-significant SSC designation."

Because the primary purpose of the RPP-WTP Project facility and collocated worker exposure standards is to identify structures, systems, and components (SSC) required to protect these workers, the guidance cited above is both applicable and appropriate.

The principal approach for complying with the 25 rem/event worker exposure standard is the PHA. The PHA is a systematic, team-based review of the plant and treatment processes. The PHA identifies hazards and operability problems to a level of detail commensurate with the design detail available. Further hazard evaluation takes place in parallel with design development to ensure that safety continues to be built into the design process.

Having generated the list of hazards and hazardous situations, this list is subject to a further systematic team-based review where a binning process takes place. The binning process assigns postulated events to a certain ~~hazard category and is essentially risk-based with categories of hazard defined according to a frequency/consequence matrix~~severity level for further detailed analysis and comparison to radiation exposure standards.

1.3.8 Acceptable Level of Worker Safety

Radiological exposure standards applied to the facility worker and collocated worker are provided in Table 1-2. The location of the workers is shown in Figure 1-3. A 5 rem/event standard is applied to the workers for anticipated events, and a 25 rem/event exposure standard is applied to workers for unlikely and extremely unlikely events. The 25 rem/event standard corresponds to the once-in-a-lifetime accident or emergency exposure for radiation workers which, by recommendation of the National Committee on Radiation Protection (NCRP 1963), may be disregarded in the determination of their radiation exposure status. In addition, an exposure of 25 rem/event corresponds to a conditional probability of fatality of about 2×10^{-2}. For unlikely events (defined in Table 1-2 as having a maximum occurrence frequency of 10^{-2}/yr), this equates to a maximum increase in worker lifetime risk of premature death of about 2×10^{-4}/yr, which is less than the average of the accidental death risk for workers in some of the safest industries, such as retail and wholesale trade, manufacturing, and service (EPA 1991).

Compliance with the 25 rem/event worker standard is established using qualitative methods of the PHA supported, where necessary, by numerical analyses that may include the development of event trees and fault trees or the performance of consequence analyses. From this process, preventative and mitigative engineered and administrative controls to be added to the design are identified~~. The PHA identifies hazards and operability problems based on the design detail available and experience with similar facilities. Further hazard evaluation takes place in parallel with design development to ensure that safety is built into the design process. Having generated the list of hazards, this list is subject to a further systematic team-based review where a binning process takes place. The binning process is essentially the risk-based categorization of hazards and hazardous situations according to a frequency/consequence matrix~~.

The 25 rem/event worker standard for unlikely or extremely unlikely events applies to events with frequencies less than 10^{-2}/yr. For those frequencies, the PHA assigns serious and major hazardous situations as either undesirable, acceptable with controls, or acceptable. For a hazardous situation to be acceptable, the situation must have consequences less than 25 rem. Where there is uncertainty concerning the appropriate hazard category to be assigned, the hazard is binned to the higher category to ensure that the accident analysis remains conservative.

For those accidents that involve a radionuclide release, the calculated exposures are compared to the radiological exposure standards of Table 1-2 to determine the need for accident prevention or mitigation features credited for worker safety. For chemical release, the projected exposure is compared to the standards in ERPG-2. If the analysis of radiological or chemical exposures do not confirm the adequacy safety, the need for engineered or administrative controls to prevent or limit the release is addressed. These features are designed and maintained to the highest applicable standards to ensure their functional performance in the prevention or mitigation of accidents. Features credited for satisfying the radiological exposure standards of Table 1-2 and chemical release exposure standards of ERPG-2 (AIHA 1988) are classified as Safety Design Class.

3.0 Conformance to Top-Level Safety Standards and Principles

This chapter discusses the methods used to conform to top-level safety standards and principles. The top-level standards and principles include any of the safety standards or principles established in DOE/RL-96-0006, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors* (DOE-RL 1996b). Among the many topics covered in the following sections are defense-in-depth, quality assurance, safety culture, training and qualification of personnel, emergency preparedness and internal safety oversight. Integrated Safety Management Plan (ISMP) Section 4.1.1, "Development of the Safety Requirements Document", provides additional information on how the top-level safety standards have been addressed for the Project.

3.1 Defense-In-Depth

Implementation of Defense in Depth for the RPP-WTP is provided in SRD Volume II, Appendix B, "Implementing Standard for Defense in Depth".

3.1.1 Approach to Defense-in-Depth (this section has been deleted)

~~The BNI approach to the control of hazardous situations is by prevention and mitigation. Prevention of hazardous situations takes place either by removing the hazard or hazardous situation by design (for example, by substituting a non-hazardous chemical for a hazardous chemical) or by providing administrative and engineered controls such that the frequency of the hazardous situation is acceptably low. Mitigation of hazardous situations is accomplished by providing reliable and robust protection such that, if the hazardous situation were to occur, its consequences would be acceptably low. This reliability and robustness is achieved, in part, by the preference for passive engineered features with their inherent safety. Administrative controls for accident prevention include training and procedures related to normal operation and facility maintenance and the commitment to a strong safety culture (Section 3.4 "Safety/Quality Culture"). Engineered features that enhance accident prevention and mitigation include application of proven engineering practices (Section 3.7, "Proven Engineering Practices").~~

~~BNI uses a deterministic approach to control hazardous situations. This is accomplished in tandem with the evolving design. Early recognition of hazardous situations when the design is most flexible allows maximum use of this approach. Where hazardous situations cannot be removed by design, protection is identified to prevent or mitigate the hazardous situation. The degree of protection applied is commensurate with the consequence and frequency of the hazardous situation. Defense-in-depth means that multiple layers of protection are applied against the hazardous situation such that no one layer of protection is completely relied on to ensure safe operation of the facility. The number of layers of protection, or barriers, is dependent upon the severity (i.e., consequence) of the hazardous situation to be prevented or mitigated. The analysis to show compliance to the accident risk goals (SRD Safety Criteria 1.0-3 and 1.0-5) may identify the need not only for additional barriers to satisfy the accident risk goals, but also to achieve additional defense-in-depth. One aspect of defense in depth is that no single failure of protection will allow a hazardous situation to occur. Protection is either passive or active; passive protection features are inherent features of the design that provides protection without the need for any action (e.g., shielding).~~

~~An element of the line of defense against the occurrence of hazardous situations is training and procedures that serve to reduce the probability of operator error and facilitate prompt and proper operator response to offnormal conditions. This prompt and reliable operator response serves to reduce the challenges to preventative and mitigative engineered safety features.~~

~~While operator response is an element of defense-in-depth in achieving effective mitigation of accident conditions, in the evaluation of the consequence of accidents to the chemical and radiological exposure standards, credit is normally taken only for engineered features.~~

~~When offnormal situations occur, the protection against release of radiological and chemical materials is ensured through multiple confinement barriers. Primary confinement is the process vessels, piping, and the dedicated process vessel ventilation system (with filtration). Secondary confinement is the cell or glovebox and its ventilation system. Tertiary confinement is provided by the operating corridor outside the cell together with another dedicated ventilation system. Design features that reduce exposure are conservatively assessed to ensure adequate protection against hazardous situations.~~

~~Design features that offer defense against the potential for exposure include shielded maintenance areas (bulges), ventilation systems providing filtered release, and area radiation and airborne monitoring systems that warn personnel of changing or unsafe conditions.~~

~~The application of the requirements of the quality assurance program during design, procurement, construction, commissioning, inspections, operations, maintenance, and modifications provides assurance that the engineered and administrative controls perform as required. Surveillances of specific project activities are conducted to determine compliance of in-process activities to quality assurance program requirements. Performance monitoring is used to verify that the necessary programs, plans, and procedures are established and implemented to ensure that activities are maintained in compliance with the applicable requirements.~~

~~Emergency preparedness is the final element of the Project approach to defense-in-depth. Emergency preparedness provides assurance that, should a significant radiological and chemical release occur, prompt action can be achieved to limit the exposure to the public and workers. Emergency preparedness includes emergency plan implementing procedures as administrative controls and instrumentation to detect and monitor the progression of accidents as engineered features.~~

~~Defense-in-depth is applied by specifying that protection against a hazardous situation is always a combination of engineered features and administrative controls providing prevention and mitigation. This means that excessive reliance is not placed on any one system to provide the majority of protection. Each protection system (i.e., mitigative or preventative, engineered, and administrative) provides the required degree of protection on its own. The design process bins hazardous situations according to their assessed consequences and frequency, which results in obtaining a hierarchy of hazardous situations according to their severity. The more severe the hazardous situation, the greater the level of protection specified. For hazardous situations identified as having the potential to exceed the public or worker exposure standards, certain engineered features are designated as Safety Design Class (see ISMP Section 1.3.10, "Classification of Structures, Systems, and Components"). These engineered features are subject to additional design, quality assurance, operational, and maintenance requirements adding confidence in their ability to perform their specified safety function.~~All text on this page has been deleted.

All text on this page has been deleted.~~An example of the application of defense-in-depth is the protection provided against entry into a melter maintenance room when the melter cell shield door is open. The first line of defense against such entry is training and procedures. The training informs personnel of the high radiation field present when the melter cell shield door is open and the procedures to be followed for entry into the melter maintenance room. Procedures are used to control entry into a melter maintenance room including the use of a personnel access door key lock. Engineered features that protect against inappropriate entry include a door interlock that inhibits entry when a high radiation field exists in the maintenance room.~~

~~Facility design germane to defense-in-depth typically includes SSCs that function as the following:~~

~~1)Barriers to contain uncontrolled hazardous material or energy release~~

~~2)Preventative systems to prevent hazardous situations and to protect barriers~~

~~3)Systems to mitigate uncontrolled hazardous material or energy release given barrier failure~~

~~4)Interlocks and controls to prevent hazardous situations~~

~~5)Indication and alarms that warn of the occurrence of hazardous situations~~

~~6)Interlocks and controls to prevent access to high radiation sources~~

~~Administrative controls are linked to the overall safety management programs that directly control operation. Administrative features include the following aspect of operator interfaces:~~

~~1)Procedural restriction or limits imposed~~

~~2)Manual monitoring or critical parameters~~

~~3)Equipment support functions~~

~~In addition, risk analyses are performed to confirm that facility accident risk goals of *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006 (DOE-RL 1996b) are met. These risk analyses may show that certain events are significant contributors to the overall accident risk. Additional defense-in-depth items will be specified to reduce that risk. Conversely, if the risk assessment identifies areas of excessive conservation, unnecessary controls may be removed.~~

~~In summary, defense-in-depth is applied in the following manner:~~

~~1)Conservative identification of the hazardous situation~~

~~2)Conservatism is applied in assessing design features for normal operations such that they also provide protection against hazardous situations~~

~~3)If the hazardous situation cannot be eliminated from the design the potential consequence of the hazardous situation is conservatively assessed. This can be qualitative assessment (use of a binning matrix and judgement) or a quantitative frequency and consequence calculations if deemed appropriate~~

~~4)Use of operator training and procedures as an element of defense-in-depth (i.e., the operator responds appropriately to the development of a hazardous situation to return the facility to normal operation or to place the facility in a safe state)~~

~~5)The combination of engineered features and administrative controls provided depend on the overall severity class of the hazardous situation~~

~~6)If the potential for exceeding the public or worker radiological or chemical exposures standards exists, Safety Design Class engineered features are specified~~

~~7)Application of the quality assurance program to design, procurement, construction, and operation to provide additional assurance that administrative and engineered controls are effective~~

~~8)Emergency preparedness to provide assurance that, should a significant radiological and chemical release occur, prompt action can be achieved to limit the exposure to the public and workers~~

~~Implementation of defense-in-depth for the Project is accomplished by the *Implementing Standard for Defense In Depth*.~~

3.2 Safety Responsibilities

BNI recognizes its corporate responsibility for safety during the design, construction, and commissioning (DC&C) phase of the project. Safety responsibilities are assigned to and by the Project Manager. The DC&C responsibilities are assigned to functional areas as shown in ISMP Tables 9-1 through 9-3. The roles assigned to organizations are provided in ISMP Chapter 11.0, “Organization Roles, Responsibilities, and Authorities”. By these assignments, facility safety becomes a facility-wide responsibility with safety responsibilities identified for each functional area.

In addition, by these assignments, assurance is provided that the roles identified in the Safety Analysis Reports are carried out.

The Facility design is based on the design and operational experience gained at other nuclear and chemical facilities. As such, the potential hazards are well understood and lessons learned from earlier facilities are applied.

The engineered features are designed and maintained to the highest applicable standards to ensure their functional performance in the prevention and mitigation of accidents. Recognized and accepted consensus codes and standards are used. Features credited for satisfying the public and worker radiological and chemical exposure standards of SRD Safety Criteria 2.0-1 and 2.0-2 are classified as Safety Design Class. Details on the classification process and the quality assurance provisions provided for each classification are provided in ISMP Section 1.3.10, "Classification of Structures, Systems, and Components", and Section 1.3.11, "Quality Levels". Additional information on the design of SSCs credited for worker and public protection is provided in ISMP Sections ~~3.1, "Defense-in-Depth",~~ 3.7, "Proven Engineering Practices"~~,~~ and 3.11, "Safety Systems Design", and in SRD Volume II, Appendix B, "Implementing Standard for Defense in Depth".

A specific list of SSCs credited for worker and public protection is provided in ISAR Section 4.8, "Controls for the Prevention and Mitigation of Accidents". These SSCs are identified in the master equipment list, which is maintained by the Configuration Management Program as discussed in ISMP Section 5.3, "Configuration Management".

3.7 Proven Engineering Practices

The RPP-WTP design incorporates the use of proven technologies so that lessons learned from the use of the technology is incorporated into the operation of the facility. For the novel uses of existing technologies (such as the use of specific ion exchange resins), the PHA ensures that the safety aspects are examined in a structured research and development program to be assured that hazard potentials are reduced as far as practicable or that protection put in place is commensurate with the assessed magnitude of the hazard.

Facility processes are based on selected technologies that minimize the risk of radiological and chemical exposure. For example, sampling and maintenance activities do not require breach of confinement; hands-on maintainable items within active areas are accessible via shielded access areas that have decontamination facilities installed; and samples with high activity levels are dispensed and transported remotely.

New and novel uses of existing technologies and processes are employed to enhance the process while maintaining safe operation. These uses (e.g., selection of ion exchange resins and the melter feed processes) are examined through a program of research and development. Such development work includes operating a pilot (cold operation) melter and associated feed and mechanical handling systems. This prototype is used to examine and prove novel processes, test the design and maintainability of components, and provide operator training in operational and maintenance activities. To support the use of new and novel uses of existing technologies and processes and new equipment, it may be necessary to develop ad hoc standards. ~~The use of ad hoc standards is discussed in SRD Volume I, Section 3.4.2, "Identification of Consensus Codes and Standards"~~Standard development is in accordance with established engineering practices and company procedures governing development of RPP-WTP documents.

The RPP-WTP design incorporates passive and active engineered features that prevent and mitigate the potential for radiological and chemical exposures to the public, worker, and the environment. In the selection of required controls, preference is given to accident prevention over mitigation and engineered features over administrative controls. Preference is also given to passive engineered features over active

engineered features. The designation of safety features is made during the hazard evaluation and accident analysis processes.

Examples of passive and active features are described in the following sections.

3.7.1 Passive Features

Facility processes are confined by at least two barriers. Facility and process equipment provides the first barrier and a cell or similar enclosure provides the second. This secondary confinement barrier has appropriate levels of shielding to ensure that radiological exposure does not exceed standards. Confinement and shielding design are established, as are the codes and standards that are used. Aspects of confinement design ensure that failure of one barrier does not lead to failure of the other (i.e., confinement is diverse). For example, should a process vessel or pipework leak (loss of primary confinement), the liquor drains to the cell sump where it can be recovered. The cell is lined to prevent liquor leakage. The potential for failure of a process vessel or piping is reduced by the selection materials resistant to erosion and corrosion and the use of direct inspection or erosion/corrosion coupons as discussed in Section 3.13, "Reliability, Availability, Maintainability, and Inspectability (RAMI)".

3.7.2 Active Features

The facility ventilation systems are designed to minimize the potential for radiological and chemical release into or out of the facility. The air flow into the facility is drawn through areas designated as having low or no potential for radiological or chemical release, through areas of successively higher potential. Except for the facility ventilation systems serving areas evaluated as having marginal potential for radiological contamination, this air is then filtered before release. Ventilation systems are exhausted to the atmosphere via monitored stacks. The principles behind the design and the systems employed are tried and tested components. Additionally, important to safety ventilation systems contain redundant equipment (fans, filters, electrical supply) to protect against single active failures.

The selection of facility equipment required to perform a safety function is based on proven design. The safety performance function requires that suitable testing and maintenance regimes are in place to ensure reliability. For example, where programmable logic controllers are used, specific attention is given to their unique requirements relative to software verification and protection against electromagnetic interference (See SRD Safety Criterion 4.3-1).

Protection systems are an integral part of defense-in-depth as described in ~~ISMP Section 3.1~~SRD Volume II, Appendix B, "Implementing Standard for Defense-in-Depth".

Preference is given in the facility design to components failing in their safe position on loss of motive power. During the design process, the failure modes of safety features are determined and specified. Simple and proven items of equipment (e.g., valves and pumps) are used, the (required) failure modes of which are well understood and categorized.

Proposed changes to the SRD are evaluated for impact on safety compliance with regulations and the authorization basis (including hazard and accident analysis) and then are reviewed and approved commensurate with the process applied to the original configuration, including regulatory approval before implementing changes that could be considered as decreasing the prescribed level of safety. The essential elements of DOE/RL-96-0004 *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for TWRS Privatization*, as addressed in the original development of the SRD, are maintained, including the use of subject matter experts and the use of an equivalent level or review and approval of the proposed change. Changes are made by an established configuration management process.

4.2 Tailoring Safety Management Processes

The aspects of the RPP-WTP design that are critical to safety are identified through Process Hazard Analysis (PHA). This process is a systematic team-based review of the facility and process designs that identifies hazards and hazardous situations to a level of detail commensurate with the available design detail. Major hazards and hazardous situations are identified as the level of design detail increases and additional PHAs are performed in Part B. Having generated the list of hazards and hazardous situations, this list is subject to a further systematic team-based review where a binning process takes place.

~~Hazardous situations are assessed and binned according to a qualitative, and experience, and team-based judgement of frequency and consequence (severity). This binning process receives benefit from the BNI team's experience with safety analysis and operation. Frequency bands are defined and labeled as normal, anticipated, unlikely, and extremely unlikely. Consequences range from negligible through minor to serious and major. The binning process is essentially risk based with categories of hazard defined according to a frequency/consequence matrix. This approach is consistent with the American Institute of Chemical Engineers (AIChE) guidelines on hazard evaluation (AIChE 1992). The binning process assigns hazards as acceptable, acceptable with controls, undesirable, or unacceptable.~~

In this way, a hierarchy of hazards and hazardous situations is identified. This hierarchy is reviewed and, where possible, the design is modified to eliminate hazards. Where this cannot be done, protection systems are identified that would prevent, protect against, or mitigate the hazardous situation. Protection systems would be a combination of engineered features (e.g., alarms, trips, and interlocks) and administrative controls (i.e., operator actions).

The application of protection systems is tailored to the hazard severity. For example, high-frequency hazards with severe consequences have protection systems involving diverse engineered features and training and procedures requirements as discussed in Section 4.2.2, "Training and Procedures". Less significant hazards would require fewer protection systems that may lean heavily on administrative procedures, the importance of which will have been stressed through adequate worker training. This ensures the appropriate level of safety is provided.

7.4 Resolution of Conflicting Requirements and Standards

Conflicting standards and requirements can arise internal to the radiological, nuclear, and process safety regime and external to this regime. The Project safety management process addresses both types of conflicts as described below.

Internal Conflicts

Internal conflicts are identified as a direct consequence of the Project approach to design. The ISMP Section 4.1.3, "Development of Safety Management Programs", describes how the Safety Requirements Document (SRD) is linked to the design process to ensure that standards are properly implemented. Because all standards and requirements information flows down into lower level design guides (see Figure 4-2), internal conflicts are recognized. At this point, the process established to maintain the SRD is used to resolve the conflict. The process for maintaining the SRD is described in SRD Volume II, ~~Section 3.6~~Appendix A, "~~Maintenance of the SRD~~Implementing Standard for Safety Standards and Requirements Identification".

External Conflicts

To ensure that current regulatory requirements and regulatory changes are promptly and accurately identified, BNI team members maintain access to multiple regulatory resources, as discussed in Section 2.1.

When the potential applicability of an existing, new, or revised regulatory requirement is identified, any conflicts are resolved. The impact on project cost and schedule, along with the feasibility of implementing the requirement, are included in the evaluation.

Routine meetings with the regulator offer a forum for identification and discussion of external conflict issues. Letters between the regulating agencies and the ~~CHG~~BNI team provide formal documentation of issue resolutions.

In the cases where safety and environmental regulations conflict, absent the granting of an exemption from the regulation, the more stringent regulation is followed.

The nature of taking responsibility for operation of the double-shell tank AP-106 requires the resolution of a number of interface concerns. From an early stage, interface meetings were held among BNFL, the DOE, and the Project Hanford Management Contractor (PHMC) to identify and resolve these concerns. Interface responsibilities are agreed on and recorded in interface control documentation. Adding concerns to this documentation and accepting their resolution requires approval of all parties involved with the interface issue.

Table 1 - SRD Volume II, Appendix A – Proposed Changes
24590-WTP-ABCN-ESH-01-001, Rev. 1, Attachment 3

Section	Change	Reason
1.0	The phrase "from work identification through confirmation of standards" is added.	To make it clear the iteration aspect of ISM relates to the entire hazard analysis and standards selection process and not to just the standards selection portion of the process.
1.0	A discussion is added that not all elements of this implementing standard will be completely implemented during the initial ISM activities.	To explain that the early ISM activities will not have all elements completely defined. However, it is also explained that the process will be completed prior to; 1) receiving the Construction Authorization for design and construction issues; 2) the Operating Authorization for design, construction, and operating issues; and receiving hazardous material at the RPP-WTP.
1.0	Editorial changes are made to the third paragraph.	Write as "resulting from" and "as needed."
2.0	Revise first paragraph regarding the resources required to perform the ISM activities.	Separate the issue of adequate resources (which includes more than people with the right background [e.g., computers, databases, documentation, and meeting facilities) from the issue of having sufficient people with the right background.
2.0 and others	In several locations in the Appendix A changes have been made to reference "ISM Teams" in lieu of other terms such as "integrated teams."	To refer to the teams in a consistent manner and using the term that is being used by the RPP-WTP.
2.0 and 4.0	Reworded to explain that ISM is usually conducted on a plant system.	There may be situations for which the hazard analysis is not performed on a defined plant system (e.g., the handling of hazardous packaged materials on a loading dock).
2.0	Address updating of the process hazard analysis	Text needs to be added as Appendix A will be the implementing standard for SRD SC 3.1-7.
3.0	Editorial change.	Capitalize "Work."
3.0	Remove reference to the documentation of the results of the identification of work activity.	Section 4.9 deals with documentation of the results of the hazard evaluation, including the results of work identification. There is no need to mention this in two places.
3.0	Remove the statement that work identification is an iterative process and is reconsidered later as a result of the outcome of other activities.	This is iterative aspect of the ISM process is addressed in the proposed addition to the second paragraph of Section 1.0. "Introduction."
4.1	Replace the term "workers" with "facility and collocated workers."	Near the end of Part A BNFL agreed with the RU that facility and collocated workers would not be lumped as "workers" when making reference to exposure standards. Also, as "worker" is defined in DOE/RL-96-0006 it excludes the collocated worker (i.e., "Worker means an individual within the controlled area of the facility performing work for or in conjunction with the Contractor or utilizing Contractor facilities").
4.2	Editorial change.	Add "those resulting from." Common mode and common cause failures by themselves usually are not accidents.

Section	Change	Reason
4.3.1	In the first paragraph clarify when credit should and should not be taken for SSCs in the assignment of severity levels.	To make it clear at the very beginning the confirmation of severity levels is based upon bounding unmitigated releases. Added that severity level assignments may credit the contribution that a cell or cave contributes to a leak path factor, limitation of spilled liquid pool size, or plateout when the credited aspect is not challenged by the event.
4.3.1	Rewrite the penultimate paragraph to focus on the assignment of severity levels assignments based upon quantitative consequence analysis and qualitative assessment.	The standard needs to separate the performance of consequence assessments for the purpose of confirming severity levels (which is performed early in the ISM process) from the performance of consequence assessments for the analysis of DBEs (which is performed later in the process). As the paragraph is written it confuses these two analyses.
4.3.1	Remove reference to a graded application of the PSM rule.	If the RPP-WTP comes under the provisions of the PSM rule (29CFR1910.119), then the rule must be complied with completely (absence the granting of an exemption). Reference to ERPG-2 for implementation of the rule is not appropriate as it is not a criterion of 1910.119(a) for application of the rule.
4.3.2*	Delete reference to “formal” accident analyses.	All accident analyses required of the RPP-WTP are “formal” accident analysis in that they are performed by qualified individuals according to procedures with the results documented as QA records.
4.3.2*	Delete the listing of the types of internal events considered.	The listing is that of typical events considered in facilities such as the RPP-WTP. The accident types that are actually applicable to the facility are identified by the hazard analysis performed for the facility. It is not believed that it is necessary to list typical events in the implementing standard.
4.3.2*	Delete the listing of factors to be considered in the accident analyses.	The listing mixes radiological release, direct radiation exposure, and chemical release events. Appendix A has now been revised to address these accidents separately. However, this detail has not generally been relocated to these new sections as this level of detail (i.e., listing the factors to be considered in accident analysis) is more appropriate for the accident analysis procedure.
4.3.2*	Relocate what remains of Section 4.3.2 to Section 4.6.	Much of what remains of Section 4.3.2 is already provided in Section 4.6 and there is no reason to discuss the definition and the analysis of DBE in separate sections. Also, it is more appropriate to discuss the performance of DBE analyses after the discussion of normal conditions and common mode and common cause events which in the ISM process come before the performance of DBE analysis.
4.3.2* and elsewhere	Change to read as “preferred hazard control strategies.”	For clarity, the first appearance of reference to control strategy development in a paragraph of Appendix A uses the full term “preferred hazard control strategy” or “potential hazard control strategy.”

Section	Change	Reason
4.4	Change the title of Section 4.4 from "Estimate of Accident Frequencies" to "Estimate of Event Frequencies."	The term "event" describes a broader set of conditions to be analyzed. Reference to "accident frequencies" could be interpreted to refer only to DBEs.
4.4	Change to state that as the design matures information on the frequency of hazardous events may be gained by use of the listed techniques (rather than "will be gained").	There may be some initiation events for which it will be difficult to develop additional information on the initiating event frequency.
4.4	Remove reference to HAZOP and FMEA as means of developing frequency of occurrence estimates.	As HAZOP and FMEA are not quantitative processes they usually are not of assistance in estimating frequencies of occurrence.
4.5	Revise the presentation of common mode and common cause failures.	This change is to bring the nomenclature into conformance with the terms and definitions currently in general acceptance throughout the risk and reliability community and eliminate confusion as to the actual meaning of "common mode" and "common cause" designations for multiple failure events. This process is consistent with the definitions of common mode and common cause failures included in DOE/RL-96-0006 and is consistent with the requirements of Section 4.2.2.2 of DOE/RL-96-0006.
4.6	Change the section title to "Selection and Analysis of Design Bases Events".	It is proposed to relocate DBE analysis requirements from Section 4.3.2 to Section 4.6 for the reasons stated above (for Section 4.3.2). "Selection" is a better term than "definition" for describing the process of identifying the DBEs to be analyzed.
4.6	Add mention in the first and second sentences to 1) identification of internal hazards and hazardous situations, 2) selection of DBEs, and 3) the establishment of performance requirements for prevention and mitigation SSCs.	The selection of DBEs depends upon the identification of both hazards (e.g., the existence of anhydrous ammonia) and hazardous situations (e.g., adding the wrong chemical to a tank of anhydrous ammonia). An editorial change in that "establish" is a better term than "define"
4.6	In Section 4.6 and elsewhere make changes to correctly refer to "hazards" and "hazardous situations."	The term "hazard" refers to the existence of a source of danger (material, energy source, or operation). The term "hazardous situations" refers to a scenario made possible by the existence of the hazard that could be challenging to humans or the environment.
4.6	Add the statement that analysis of DBEs provides confirmation that the requirements of SRD SC 2.0-1 and 2.0-2 are satisfied.	With the proposed deletion of Section 4.3.2 this needs to be added to Section 4.6.
4.6	Editorial changes to the second paragraph.	Reinforce that DBEs for internal hazards and hazardous situations are being addressed and "establish" is a better word than "define."
4.6	Delete the third paragraph.	The fact that the ISM Team identifies internal and external events is addressed in the first two paragraphs.

Section	Change	Reason
4.6	Add clarification that the SRD includes natural phenomena loads rather than just list natural phenomena events.	As written it sounds like the SRD only lists NPH events (e.g., straight wind) rather than also provide NPH loadings (e.g., a straight wind of 91 mph, 3 second gust, at 33 feet).
4.8	State that the ISM Team shall identify one or more potential hazard control strategies.	As currently written it could be implied that the ISM Team must identify several potential hazard control strategies. While in most cases the ISMP Team does develop several potential hazard control strategies, in some cases they might develop just one (e.g., if the strategy is obvious or the options limited).
4.8	Explain that the ISM Team develops potential hazard control strategies for those cases where unacceptable consequences might result from the hazardous situation.	The ISM Team does not need to develop potential hazard control strategies for events for which the unmitigated consequences do not challenge the exposure limits.
4.8	In Section 4.8 and elsewhere refer to "potential hazard control strategies" and "preferred hazard control strategies" in a consistent manner.	Potential hazard control strategies are developed by the process defined in Appendix A, Section 4.8. Preferred hazard control strategies are selected by the process defined in Section 5.0.
4.9	Re-title Section 4.9 as "Documentation of the Hazard Evaluation."	Section 4.9 only concerns documentation of that portion of the ISM process discussed through Section 4.8. Documentation of the subsequent activities is discussed later in the individual sections of Appendix A.
4.9	Revise the first paragraph of Section 4.9 to make it clear that the HAR or SAR includes the results of the hazard evaluation and the hazard database includes or reference the results of having conducted the various steps of the hazard evaluation.	As written it is unclear what part of the hazard evaluation is included in the HAR or SAR. Relative to the database, the sentence could be interpreted as only requiring that the database include the results of the hazard evaluation (although the listed items that follow make it clear the database is to include more than this). The change also allows for the database to reference where information is available rather than require that the information be included in the database. Reference to the SAR is added as for the CARs the submittal of a revision to the HAR is not required. However, reference to the HAR is retained at this time as, until the CARs are approved, the HAR remains as the documents that includes this information.
4.9	Editorial changes to list of items included in the hazard database.	Clarify that the assumptions made with regard to the severity level assignment is what is important.
4.9	State that the process of conducting the hazard evaluation is described in the HAR or SAR and not the SRD.	Reference to the SRD was incorrect. The SRD includes the results of the selection of standards following the hazard evaluation process. However, the methodology for performing the hazard evaluation should be provided in the HAR or SAR

Section	Change	Reason
4.9	Delete reference to "description of results" in the listed items.	As Section 4.9 is to be revised (see above change) this listing is the contents of the HAR or SAR and the requirement that the HAR or SAR include the results of the hazard evaluation is covered by the first sentence of Section 4.9 as proposed for revision.
5.0 and elsewhere	Change the title of Section 5.0 to "Development of Preferred Hazard Control Strategies."	For clarity, the first appearance of reference to control strategy development in a paragraph of Appendix A uses the full term "preferred hazard control strategy" or "potential hazard control strategy."
5.0	Clarify that SRD Appendix B on defense in depth includes both requirements and goals.	It is incorrect to imply that the SRD Appendix B implementing standard only includes guidance.
5.0 and 7.0	Explain the "operating environment" includes such items and temperature and humidity.	To make certain it is understood that "operating environment" refers to environmental conditions that might challenge the operability of a system or component.
5.0	State that the degree to which a preferred control strategy complies with the listed factors and elements is documented in the SAR.	Currently the appendix does not identify where implementation of this portion of the ISM process is documented.
5.0	Explain that the preferred control strategies are evaluated for the most bounding conditions (i.e., the most demanding requirements imposed by the set of hazardous situations that credit the function of the control strategy)	To make it clear that consequence analyses are not performed for all events that require a SSC for prevention or mitigation.
5.0	Add reference to "hazardous situation" in two locations.	The selection of preferred hazard control strategies is dependent upon the hazards in the facility and the identification of the hazardous situations the presence of these hazards can lead to.
5.0	Explain that the estimate of the consequence of the mitigated events and event frequency result from the performance of DBE analyses.	To make it clear that this aspect of preferred hazard control strategy development comes as input to the ISM Team from another activity.
5.1, 5.2, and 5.3	Provide three sections that separately address radiological release events, direct radiation exposure events, and chemical hazards.	Currently Appendix A does not serve as a standard for addressing direct radiation and chemical exposure events.
5.1	Explain that the process vessels and piping <u>usually</u> form the primary confinement barrier and that the cells and ventilation system <u>usually</u> form the secondary confinement barrier.	Some events, such as out-of-cell events, do not have all of these listed features as confinement barriers.

Section	Change	Reason
5.1	After the sentence "These target frequencies may be used to guide control strategy development as described below," the following sentence is added "In all cases the control strategy development must conform to SRD Safety Criterion 2.0-1."	To explain that while the target frequencies are a guide to be used in developing control strategies, the control strategies must ensure compliance with the exposure standards of SRD Safety Criterion 2.0-1.
5.1	For SL-1 events combine the first, second, and fourth bullets.	These items all deal with application of the single failure criterion.
5.1	For SL-1 events revise to explain that SSCs credited for meeting the radiological exposure standards shall satisfy the single failure criterion as discussed in SRD Volume II, Appendix B.	The first bullet as currently written implies that implementation of the SFC is driven by the need to meet the target frequency. In fact, the need to impose the SFC is mandated independent on the need to meet the target frequency (but of course implementing the SFC will assist in meeting the target frequency). Added reference to Appendix B to clarify the reference to the Implementing Standard for Defense in Depth.
5.1	For SL-2 events explain the meeting the target frequency may require diverse and independent SSCs rather than state that such SSCs are usually required.	It is expected that in many cases single failure protection will not be required to meet the SL-2 target frequency.
5.1	For SL-2 events delete the third bullet that SL-2 events should satisfy the single failure criterion in the Implementation Standard for Defense in Depth (Appendix B).	Application of the SFC should only be imposed on SL-2 events when required to meet the target frequency. Not mandating application of the SFC for SL-2 events is consistent with Appendix B, Table 1which states for SL-2 events, " Application of the single failure criterion may be required of prevention and mitigation controls to meet the target frequency."
5.1	Replace "Notwithstanding the forgoing guidance…." with "An exception to the above guidance…."	Editorial change; The term "notwithstanding" is not always well understood in this usage.
5.2	This section added to provide a standard for addressing direct radiation exposure events.	Requirements for addressing direct radiation exposure events are currently missing from Appendix A.
5.3	This section added to provide a standard for addressing chemical exposure events.	Requirements for addressing direct chemical exposure events are currently missing from Appendix A. The first paragraph is a copy of what is currently included in Section 4.3.1.

Section	Change	Reason
6.0	Replace details on the classification or SSCs with a reference to SRD Safety Criterion 1.0-8.	Safety Criterion 1.0-8 provides this information of classification and it is best to only provide this information in one location in the SRD. In addition ABCN 24590-WTP-ESH-01-001-029 proposes changes to the classification of SSCs. With this proposed changed to Appendix A the appendix will be transparent to the change proposed in ABCN 24590-WTP-ESH-01-001-029.
6.0	Replace details on the attributes of Safety Design and Safety Significant SSCs with a reference to the Quality Assurance Program.	The Quality Assurance Program provides this information on classification and it is best to only provide this information in one authorization basis document.
7.0	Explain that the ISM Team that identifies standards may not be the same team that performed the work identification and hazard analysis.	Because of differences in the expertise required, the makeup of the ISM Teams may differ for the different aspects of the ISM process.
7.0	Add reference to the technical staff of the Area Managers.	To reflect the current organization.
7.0	Editorial change.	Explain that the data is retained in one or more databases.
7.0	Replace reference to “hazard schedule” with “hazard evaluation records”.	The “hazard schedule” term may not be understood; it is UK terminology.
7.0	Remove the statement that the standards identified as reflected in the SRD.	Documentation of the results of the standards selection in the SRD is addressed in Section 9.0. Section 9.0 states that the results of the standards selection process shall be documented in the SRD.
10.0	Add the word “and” to the second item listed.	To make it clear that all three items must always be satisfied.
11.0	Add new section 11.0, SRD Maintenance. Change Section 11.0 and 12.0 to 12.0 and 13.0 respectively.	To incorporate discussion on SRD maintenance (including material relocated from SRD Volume I, Section 3.6) to make Appendix A complete.
11.0	Add new figure A-1, SRD Compliance Process	As SRD Volume I is to be deleted, this figure needs to be relocated from Volume I, Section 3.6. The figure provides clarification of the SRD Compliance Process.
12.0	Add a definition of dependent failures.	To support the discussion added to Section 4.5.
12.0	Add to the definition of the Mitigated Event Frequency the following “…is the product of the corresponding….”	To have the definition read in a manner that is parallel to the definition of the Release Frequency.
12.0	Delete the word “times” in the definition of “Release Frequency.”	Editorial change. It is better to state that a dependent variable is “…the product of A and B…” and not “…the product of A times B...”

Section	Change	Reason
13.0	Add references for AIChE 1992, the QAM, DOE/RL-96-0006 and 00004, and Modarres 1993.	Previously AIChE 1992, the QAM (QAP), 0006, and 0004 were called out in the text but not included in a list of references. The last reference is added to support proposed added dependent failure discussion to the appendix.

* This is Section 4.3.2 of the current SRD.

Section	Change	Reason
1.0	Add reference to DOE/RL-96-0006 as a source of definitions and move the "(Ref 5.4)" to the first reference o f 0006 .	The definitions for "important to safety" and "safety function" in Section 4.0 are from DOE/RL-96-0006.
2.0	Delete reference to consensus standards.	The term "consensus standards" usually refers to standards issued by such groups as the IEEE and ASME that involve participation from a number of independent organizations. Not all of the standards listed in Section 2.0 would be considered to be consensus standards.
2.1.2	Use the term "layer(s)" in several places rather than "level(s)" in the discussion of defense in depth.	The word "layers" is used in the reference (DOE O 420.1) and there is no reason to deviate from the reference.
2.1.2, 2.5.2	Replace "workers" with "facility and collocated workers."	Near the end of Part A BNFL agreed with the RU that facility and collocated workers would not be lumped as "workers" when making reference to exposure standards. Also, as "worker" is defined in DOE/RL-96-0006 it excludes the collocated worker (i.e., "Worker means an individual within the controlled area of the facility performing work for or in conjunction with the Contractor or utilizing Contractor facilities").
2.1.2	~~Delete the requirement to apply the single failure criterion to all active SSCs required to achieve defense in depth.~~ Revise to state "When the single failure criterion is implemented, it is done in accordance with …."	~~The requirement to apply the single failure criterion to all active SSCs required to achieve defense in depth is inconsistent with other portions of Appendix B and with Appendix A of SRD Volume II. The single failure criterion is imposed on control options for SL-1 events by Table 1. For SL-2 events it is adopted when necessary to meet the target frequency.~~ Response to ABCN Revision 0, Question ABCN-ESH-01-001-6.
2.1.2	Add the explanation that the single failure criterion is required of ~~active~~ prevention and mitigation controls credited for meeting exposure standards for SL-1 events and that it may be required for SL-2 events to meet the target frequency.	To make it clear that the ~~single failure criterion need not be applied to passive components. Consideration for passive single failures is more appropriate for nuclear power plants that have high and moderate energy systems required to maintain long term cooling. Also to make it clear that the~~ application of the single failure criterion is required for SL-1 controls credited for meeting the exposure standards and may be required of SL-2 events for meeting the target frequency.

Section	Change	Reason
2.1.2	Delete the discussion about application of the single failure criterion beginning with the identification of an initiating event.	Application of the single failure criterion is mandated for active prevention and mitigation controls credited with meeting exposure standards for SL-1 event. For SL-2 events it is adopted when necessary to meet the target frequency.
2.1.2	Delete the requirement to apply the single failure criterion to passive SSCs.	Consideration for passive single failures is more appropriate for nuclear power plants that have high and moderate energy systems required to maintain long term cooling.
2.2.2	Add discussions of the siting and conservatism of design aspects of defense in depth.	These are listed in Section 2.2.2 as elements of defense in depth but they are not addressed in the appendixAppendix B.
2.2.2	Remove the illustration of differences between hazard elimination and provisions for passive or active protection.	The standard does not require an example and the example provided is one of eliminating a hazardous situation rather than removing a hazard.
2.4.2	Add reference to the radiological exposure standard (RES) in the mitigated event discussion.	To make it clear that mitigation, as a minimum, must be adequate to achieve compliance with the RES.
2.4.2	Delete the constraint that credit will not be taken for tertiary confinement.	Credit should be allowed for tertiary confinement if adequate standards have been identified that provide for adequate safety and the confinement is to be designed, constructed, operated, and maintained to these standards.
2.65.2 3.1	Add a reference to SRD Volume II, Appendix A for the definition of the severity levels.	As written, Appendix B states that severity levels are to be established but it does not define them or provide a reference for their definition.
2.5.2	Revise the administrative controls discussion to mention monitoring of normal plant condition and equipment status.	The administrative control aspect of defense in depth as related to operation begins with maintaining the plant within it normal operating parameters.
2.6.2, 3.0	Indicate that the hazard control strategies contribute to defense in depth.	As currently worded the appendix implies that control strategies alone establish defense in depth.
3.0	Add reference to SRD Volume II, Appendix A and explain that the two appendices used to together contribute to defense in depth.	Aid the reader in being clear that Appendix A is the other standard being discussed and that the two appendices need to be used together to implement defense in depth.
3.0	Add a statement that satisfying the accident risk goals (SRD SC 1.0-3 and 1.0-5) may require additional controls.	This addition to Appendix B is proposed to facilitate removal of the defense in depth discussion from ISMP Section 3.1.1 (see Table 4).

Section	Change	Reason
3.1	Explain that the hazard control strategy being addressed is the "preferred hazard control strategy."	As proposed for revision, Appendices A and B use consistent terms for "potential hazard control strategy" and "preferred hazard control strategy."
3.1	Add to this section clarification that the section applies to uncontrolled release of radiological materials.	Separate sections have been proposed for radiological release, direct radiation, and chemical release events. Mention of "uncontrolled release" makes it clear that the section does not deal with normal radiological release.
3.1	Add explanation that severity and target frequencies are a tailored approach that contributes to achieving defense in depth.	As currently worded the appendix implies that control strategies alone establish defense in depth.
3.1	In the text and in Table 1 add explanation that for SL-1 events the single failure criterion is applied to ~~active~~ the set of two or more barriers ~~systems and components~~ credited for meeting exposure standards.	To make it clear that the ~~single failure criterion need not be applied to passive components. Consideration for passive single failures is more appropriate for nuclear power plants that have high and moderate energy systems required to maintain long term cooling. Also to make it clear that the~~ application of the single failure criterion is limited to those ~~active~~ engineered features credited for meeting exposure standards and that the single failure criterion does not need to be applied individually to each barrier.~~.~~
3.1	In the text and in Table 1 a~~A~~dd explanation that for SL-2 events application of the single failure criterion may be required to meet the SL-2 target frequency.	Currently the discussion does not provide this important guidance on when the single failure criterion may be required.
3.1	Delete the discussion of physical barriers for SL-1 and SL-2 events and the explanation that the discussion of barriers does not apply to direction radiation events.	This discussion of barriers for SL-1 and SL-2 events is a repeat of what is in Table 1. It is no longer necessary to explain that the discussion does not apply to direct radiation events as the new Section 3.1 clearly applies only to radiological release events.
3.1	Delete the sentence that addresses SL-4 events and 10 CFR 835.1001.	This is a repeat of what is in Table 1.
~~3.1~~	~~In two places explain that the event frequency being discussed is the "unmitigated event frequency."~~	~~These are the "initiating event frequency" and the "unmitigated event frequency". The frequency being discussed is the "unmitigated event frequency" (i.e., the product of the initiating event frequency and the probability that the control strategy will fail leading to unmitigated consequences).~~
3.1	Add an explanation that the selection of controls satisfies one aspect of defense in depth.	As currently worded the appendix implies that the implementation of control strategies alone establishes defense in depth.

Section	Change	Reason
3.1	Add to Table 1 the explanation that administrative controls alone may be credited as the controls that protect facility workers.	This explanation currently exists in the text of Section 3.1. As it is an important qualifier to Table 1 it has been added to the table.
3.1 3.2	Add to Table 1 and include in new Table 2 the following footnote "Physical barriers are not required for those events that are prevented (i.e., the product of the initiating event frequency and the conditional failure probability of the prevention system(s) is less that 1.0^{-5}/yr)."	To make it clear that events thar are prevented to not require mitigation controls. this addition was include in the revision to Question Response ABCN-ESH-01-001-13.
3.2	Add Section 3.2 on direct radiation events.	Currently Appendix B does not serve as a standard for direct radiation events.
3.3	Add Section 3.3 on chemical release events.	Currently Appendix B does not serve as a standard for chemical release events. The first paragraph is a copy of what is currently included in Appendix A, Section 4.3.1.
4.0	Revise definition of barrier.	To acknowledge that barriers also exist for direct radiation events; this revision responds to Question ABCN-ESH-01-001-19.
4.0	Add a definition of dependent failures.	The term "dependent failures" is used in the definitions of "common mode" and "common cause failures."
5.0	Revise references 5.4 and 5.14.	To address the latest revision and title change for DOE/RL-96-0006 and provide the new report number and responsible organization for the ISMP
5.0	Add reference 5.17 and 5.18.	This is the source of the definition of "dependent failures." and add DOE/RL-96-0004 which was previously cited in the text but not included in the reference listing.

Table 3 - SRD Volume II, Appendix D – Proposed Changes
24590-WTP-ABCN-ESH-01-001, Rev. 1, Attachment 5

Section	Change	Reason
2.0	Revise seventh paragraph, 2nd sentence to read "The binning process assigns postulated events to a certain severity level for further detailed analysis and comparison to Radiation Exposure Standards and Risk Goals.	Accidents are binned for subsequent DBE analysis according to their severity level (not hazard category). Accident frequencies are considered subsequent to the binning process. This change makes Appendix D consistent with Appendix A.

Paragraph	Subject	Location in SRD Volume II, Appendix B
1	Defense in depth includes prevention by removing the hazard or making the frequency of occurrence of the hazardous situation acceptably low.	Section 2.2 addresses the prevention aspect of defense in depth. Reference is not made to "making the frequency of occurrence of the hazardous situation acceptably low" as this is not a method of prevention (except for those cases where the frequency of occurrence is found or made to be less than 10^{-6} events/yr for which it is then concluded the event is prevented).
1	Defense in depth also includes mitigation by reliable and robust protection such that the consequences are acceptably low.	Section 2.4 addresses the mitigation aspect of defense in depth. The first sentence of Section 2.4.2 states that "Mitigation is implemented to ensure reduction of consequences from potential hazards and hazardous situations such that the applicable exposure standards are satisfied." This section also states that "Confinement will be achieved by physical barriers and by other SSCs that either assure integrity of the physical barriers or minimize the quantity and characteristics of any hazardous material potentially releasable." (Note changes have been made to the wording of the two quoted sentences to facilitate removal of the defense in depth discussion from ISMP Section 3.1.1). The need for reliable protection is established by the need controls to satisfy the target frequencies of Section 3.1 and 3.2. The term "robust" used in the ISMP is not proposed for addition to the SRD as the term is not defined (this relates to OSR Question ABCN-ESH-01-001-19). Tables 1 and 2 (the latter a proposed addition) provide the requirements for the barriers.
1	Mitigation also gives preference to passive controls.	Section 2.2.2 states that " Where hazard elimination is not practicable, passive features are to be employed, since they are simple and have a high degree of reliability. Where this is not practicable, active protection will be proposed that has a degree of reliability and confidence commensurate with the potential hazard severity." This section also states that "Conservatism in design is also accomplished by giving preference to passive over active components…."
1	Administrative controls for accident prevention include training and procedures related to normal operation and facility maintenance and the commitment to a strong safety culture.	Section 2.1.2 states that the first layer of defense includes "…personnel well trained in operations and maintenance and committed to a strong safety culture."
2	The degree of protection for hazardous situations that cannot be removed by design is commensurate with the consequence and frequency of the hazardous situation.	Sections 3.1 and 3.2 (new proposed section numbers) require that controls be developed based upon the severity level of the event being considered. The severity levels are dependent upon the consequences of the event. Satisfying the target frequency for a particular severity level includes consideration for the frequency of occurrence. Section 3.1 states that "After the preferred hazard control strategy has been identified, the event frequency – i.e., the product of the frequency of the initiating event and the probability that the control strategy will

Paragraph	Subject	Location in SRD Volume II, Appendix B
		fail given the initiating event – will be conservatively estimated."
2	Defense in depth means that no one layer of protection is completely relied upon to unsure safety.	Section 2.1.2 states that "…The RPP-WTP will be designed with the objective of providing multiple layers of protection to prevent or mitigate the unintended release of radioactive materials to the environment." This section also states that "This safety design strategy is based on the premise that no one layer of protection is completely relied upon to ensure safe operation." (Note the above quoted sentences are based upon changes proposed by this ABCN to replace "levels" with "layers").
2	The number of barriers is dependent upon the severity of the hazardous situation to be prevented or mitigated.	This is a requirement of Tables 1 and 2 for radiological release and direct radiation events, respectively. (Note this ABCN proposes to add Table 2 to address direct radiation events).
2	Satisfying the accident risk goals of SRD Safety Criteria 1.0-3 and 1.0-5 may require additional barriers.	Section 3.0 states "In addition to the identification of defense in depth SSCs through the implementation of SRD Volume II, Appendices A and B, the requirement to satisfying the accident risk goals of SRD Safety Criteria 1.0-3 and 1.0-5 may require the identification of additional accident prevention or mitigation SSCs." (Note this addition to Appendix B is proposed to facilitate removal of the defense in depth discussion from ISMP Section 3.1.1).
2	One aspect of defense in depth is that no single failure of protection will allow a hazardous situation to occur.	Section 2.1.2 states that "…The RPP-WTP will be designed with the objective of providing multiple layers of protection to prevent or mitigate the unintended release of radioactive materials to the environment." This section also states that "This safety design strategy is based on the premise that no one layer of protection is completely relied upon to ensure safe operation." (Note the above quoted sentences are based upon changes proposed by this ABCN to replace "levels" with "layers").
3	Training and procedures reduce the probability of operator error causing an off-normal condition and mitigating the consequences of such a condition should it occur thus reducing the challenges to preventative and mitigative engineered safety features.	Section 2.1.2 states that defense in depth includes "…the use of equipment and administrative controls which restrict deviations from normal operations and provide for recovery from accidents to achieve a safe condition…." Section 2.3.2 states that "Normal operations, which include anticipated operational occurrences and maintenance and testing activities, shall be controlled so that facility and system parameters remain within their specified operating ranges and that the frequency of demands placed on SSCs for hazard prevention and mitigation is small."
4	Relative to operator response, credit is normally only taken for engineered features.	Section 2.5.2 states that "Means shall be provided to automatically initiate and control all protective actions except as justified below. The design of important to safety systems shall be such that the operator is not required to take any action

Paragraph	Subject	Location in SRD Volume II, Appendix B
		prior to the time described below following the onset of any event (Based on IEEE Std 603-1991 – Ref. 5.11)." Credit for operator action may be permissible only if safety analysis demonstrates that the total time interval required to perform the operator action exceeds the time at which the limiting design requirement would be reached without operator action, in accordance with the methodology of ANSI/ANS-58.8-1994 (Ref. 5.7)." Section 2.6.2, states that "For the purpose of protecting the public and collocated worker, administrative controls alone shall not be relied on for the implementation of defense in depth."
5	Protection against radiological and chemical release is ensured through multiple confinement barriers; such as primary confinement (vessels, piping, and vessel ventilation), secondary (cells and glove boxes and their ventilation system), and tertiary (corridor ventilation).	Section 2.4.2 states that "The RPP-WTP will provide physical barriers to confine radioactive material and thereby prevent uncontrolled releases. In general, multiple physical barriers – i.e., primary and secondary confinement – will be provided, especially for the most severe hazards and hazardous situations."
6	Design features that offer defense against exposure include shielded maintenance areas, ventilation systems with filtered release, and area and airborne monitors.	These measures of defense against exposure need not be mentioned in Appendix B and need not be retained in the ISMP as there are simply examples of controls for direct and radiological release radiation hazards.
7	The QA program (including surveillance and performance monitoring) applied to all aspects of the project are an element of defense in depth.	Section 2.6.2 addresses the QA Manual as an element of defense in depth. Specific mention is not made of surveillances and performance monitoring in this section but reference to the RPP-WTP QA Manual is made. The manual addresses surveillances in Policy Q-18.2, Quality Assurance Surveillance. While the QA Manual also addresses some elements of performance monitoring a more complete description of performance monitoring for the WTP is provided in 24590-WTP-PSAR-ESH-01-001-01 (PSAR General Information) Section 17.4.2, Safety Review and Performance Assessments. (Note the above quoted sentences are based upon changes proposed by this ABCN; the changes are to address OSR Question ABCN-ESH-01-001-07 offered on Revision 0 of this ABCN).
8	Emergency preparedness is an element of defense in depth.	Section 2.1.2 states the defense in depth includes "…means to monitor accident releases required for emergency responses; and the provision of emergency preparedness for minimizing the effects of an accident…."
9	Defense in depth is always a combination of engineered features and administrative controls without excessive reliance on one	Section 2.6.2 states "The output of the design process, through which hazards and hazardous situations are identified, control strategies implemented and standards defined will be a set of SSCs that contribute to defense in depth. SSCs

Paragraph	Subject	Location in SRD Volume II, Appendix B
	system to provide the majority of the protection.	so identified will always be backed up by administrative controls such as procedures." The degree to which multiple systems or barriers are required for radiological and direct exposure events is provided in Appendix B Tables 1 and 2 respectively. (Note the above quoted sentences are based upon changes proposed by this ABCN to replace "achieve" with "contribute").
9	The design process bins hazardous situation according to their consequences and frequency (of occurrence). The more severe hazard receives the great level of protection.	Sections 3.1 and 3.2 (new section numbers) require that controls be developed based upon the severity level of the event being considered. The severity levels are dependent upon the consequences of the event. Satisfying the target frequency for a particular severity level includes consideration for the frequency of occurrence. See discussion for Paragraph 2 for additional details.
9	Engineered controls needed to protect against exceedence of the public or worker exposure standards are classified as Safety Design Class.	SRD Volume II, Appendix A, Section 6.0 currently addresses the classification of SSCs. This ABCN proposes that the detail of SSC classification in Section 6.0 be replaced by a simple reference to the need to classify SSCs in accordance with SRD Safety Criterion 1.0-8.
10	An example of defense in depth is protection against entry into a melter maintenance room.	This in not included in Appendix B and need not be retained in the ISMP. It is not necessary to provide an example of the application of defense in depth.
11	Facility design germane to defense in depth typically include; 1 Barriers to contain uncontrolled hazardous material or energy release 2 Preventative systems to prevent hazardous situations and to protect barriers 3 Systems to mitigate uncontrolled hazardous material or energy release given barrier failure 4 Interlocks and controls to prevent hazardous situations	These six items are addressed in Appendix B as follows: 1 Section 2.4.2 states, "The RPP-WTP will provide physical barriers to confine radioactive material and thereby prevent uncontrolled releases." 2 Preventative systems to prevent hazardous situations and to protect barriers 3 Section 2.4 addresses the mitigation aspect of defense in depth. The first sentence of Section 2.4.2 states that "Mitigation is implemented to ensure reduction of consequences from potential hazards and hazardous situations such that the applicable exposure standards are satisfied." As discussed in Appendix A, energy sources are identified relative to their available to interact with the hazardous material. (Note the above quoted sentence includes changes proposed by this ABCN). 4 Section 2.3.2 commits to "Include features to control process variables to values within safe conditions, to alert operating personnel of an approach toward conservative process limits, to allow timely detection of failure or malfunction of critical equipment, and to allow for the imposition of administrative controls assumed in the hazard analysis, and/or accident analysis (Ref 5.3)".

Paragraph	Subject	Location in SRD Volume II, Appendix B
	5 Indication and alarms that warn of the occurrence of hazardous situations 6 Interlocks and controls to prevent access to high radiation sources	5 See response for item 4. 6 Measures to prevent access to high radiation areas are not mentioned in Appendix B and need not be retained in the ISMP as there are simply examples of controls for direct radiation hazards. In response to OSR Questions ABCN-ESH-01-001-17 and -19 the procedure that implements Appendix B will be revised to address 10CFR34 and 10CFR835 for suggestions on controls for direct radiation hazards; see the ABCN entry for Item H, "List the implementation activities and the projected completion dates."
12	Administrative controls include the following aspect of operator interfaces: 1 Procedural restriction or limits imposed 2 Manual monitoring or (of) critical parameters 3 Equipment support functions.	Section 2.6.2 states "Administrative controls include features to control process variables to values within normal and safe conditions, to monitor equipment status, to alert operating personnel of an approach toward conservative process limits, to allow timely detection of failure or malfunction of critical equipment, and to allow for the imposition of administrative controls assumed in the hazard analysis, and/or accident analysis (Ref. 5.3)." (Note the quoted sentence includes proposed changes to facilitate removal of the defense in depth discussion from ISMP Section 3.1.1).
13	The risk goals of DOE/RL-96-0006 are met. This may identify additional defense in depth items to reduce risk.	Section 3.0 states "In addition to the identification of defense in depth SSCs through the implementation of SRD Volume II, Appendices A and B, the requirement to satisfying the accident risk goals of SRD Safety Criteria 1.0-3 and 1.0-5 may require the identification of additional accident prevention or mitigation SSCs." (Note this addition to Appendix B was made to facilitate removal of the defense in depth discussion from ISMP Section 3.1.1). Reference to Safety Criterion 1.0-4 is not included in Appendix B and need not be retained in Section 3.1.1 of the ISMP as this criterion deals with the risk of normal operations. The need to comply with Safety Criterion 1.0-4 is addressed in Section 3.6.1, "Normal Operations" of the ISMP and documentation of compliance to this criterion is provided in Section 3.7, [facility name] Risk Goals, of the facility-specific PSARs.
13	Conversely, if the risk assessment identifies areas of excessive conservation (conservatism) unnecessary controls may be removed.	This statement is not included in Appendix B and need not be retained in the ISMP as these documents establish minimum requirements and do not need to identify what does not need to be done.
14	In summary defense in depth includes: 1 Conservative identification of the hazardous situation	These eight items are addressed in Appendix B (or A when noted) as follows: 1 Appendix A, Section 4.3.1 imposes bounding and unmitigated assumptions

Paragraph	Subject	Location in SRD Volume II, Appendix B
	2 Conservatism in assessing design features for normal operations such that they also provide protect against hazardous situations	2 In assigning the reliability to active prevention or mitigation controls for Section 3.1 and 3.2 a higher reliability is assigned to those systems and components that running during normal operation as opposed to those that must start (and run) in response to an accident situation/
	3 If the hazardous situation cannot be eliminated from the design it is conservatively assessed.	3 Same response as to Item 1.
	4 4 Use of operator training and procedures as an element of defense-in-depth (i.e., operator responds appropriately to return the facility to normal operation or a safe state)	4 Section 2.1.2 states that defense in depth includes "…the use of equipment and administrative controls which restrict deviations from normal operations and provide for recovery from accidents to achieve a safe condition…."
	5 The combination of engineered features and administrative controls provided depend on the hazard severity	5 Section 2.6.2 states "The output of the design process, through which hazards and hazardous situations are identified, control strategies implemented and standards defined will be a set of SSCs that contribute to defense in depth. SSCs so identified will always be backed up by administrative controls such as procedures." (Note this quoted sentence includes a changed proposed by this ABCN to replace "achieve" with "contribute").
	6 If the potential for exceeding radiological or chemical exposures standards exists, Safety Design Class engineered features are specified	6 SRD Volume II, Appendix A, Section 6.0 addresses the classification of SSCs. This ABCN proposes that the detail of SSC classification in Section 6.0 be replaced by a simple reference to the need to classify SSCs in accordance with SRD Safety Criterion 1.0-8.
	7 Application of the quality assurance program to design, procurement, construction, and operation to provide additional assurance that administrative and engineered controls are effective	7 Section 2.6.2 addresses the QA Manual as an element of defense in depth.
	8 Emergency preparedness to provide assurance that, should a significant radiological and chemical release occur, prompt action can be achieved to limit the exposure.	8 Section 2.1.2 states the defense in depth includes "…means to monitor accident releases required for emergency responses; and the provision of emergency preparedness for minimizing the effects of an accident…."
15	Reference to the Implementing Standard for Defense in Depth.	This reference will be retained in Section 3.1 with specific reference to SRD Volume II, Appendix B.

Revision to Implementing Standard for RPP-WTP Integrated Safety Management Process and Defense-in-Depth

1 Purpose

The River Protection Project Waste Treatment Plant (RPP-WTP) project contract with the Department of Energy (DOE) [Ref. 1] requires that the RPP-WTP contractor maintain the Safety Requirements Document (SRD) current throughout the project. The contract also requires compliance with 10 CFR 830 and other laws and regulations. With the transition of the RPP-WTP project to the Bechtel National, Inc (BNI) design, construction, and commissioning (DC&C) contract, the implementing standard for the project Integrated Safety Management (ISM) process and Defense-in-Depth (SRD Volume II, Appendices A & B) were evaluated to determine if changes were necessary. This attachment to 24590-WTP-ABCN-ESH-01-001 documents this evaluation and updates necessary to the SRD.

2 Scope

This attachment documents the results of a specially constituted Integrated Safety Management (ISM) team for re-evaluation and identification of changes necessary to the SRD. The attachment to 24590-WTP-ABCN-ESH-01-001 furnishes a summary of an integrated safety management process for identification of these changes to the standards, rationale for the re-evaluation and identification of the standard, and documentation to demonstrate the standard meet the ISM standards selection process acceptance criteria.

In support of re-evaluation of the implementing standard for the ISM Process and Defense-in-Depth a "standards selection process", using the project ISM process, was undertaken in compliance with the DOE/RL-96-0004 [Ref. 4] regulatory process. The project-specific implementing standard for this regulatory process is detailed in Appendix A of the SRD [Ref. 2], "Implementing Standard for Safety Standards and Requirements Identification".

The identification of changes to the SRD was performed in compliance with the procedural requirements specified in project procedure K70P568 [Ref. 5]. This procedure requires that identification of standards, other than engineering/design, manufacture/fabrication, and construction standards (e.g., standards for quality assurance, conduct of operations, etc.), is performed by specially constituted teams formed by the Process Management Team (PMT).

3 Discussion

Based on the standards identification results of the ISM team and the PMT recommendation of the selected standard to the RPP-WTP Project Safety Committee (PSC) Chair, the PSC Chair requests the PSC confirm the selected set of standards. The PSC will define a confirmation review approach, carry out the review, and document the findings of the review. Comments by the PSC on standards identification will receive formal disposition by the PMT.

3.1 Approach

Upon confirmation of the ISM process-selected implementing standard by the PSC and approval by the Project Manager, based on the PSC recommendation, the implementing standard will be proposed for DOE approval of an SRD update, via the project Authorization Basis Maintenance Process.

Following approval of the ABCN by the DOE Office of Safety Regulation (OSR), the results of the standards selection ISM process will be documented in the applicable SRD safety criteria.

3.1.1 ISM Team Composition

A multi-discipline ISM team provided recommendation of an implementing standard for the RPP-WTP USQs. This team[1] consisted of the following individuals:

Name	Title	Department
John Hinckley, team chairperson	Hazards Safety Analysis, LAW Lead	ES&H/Safety Analysis
Alan Hosler	Safety and Licensing Engineer	ES&H/Regulatory Safety
Dale Lindsey	Area Program Manager	Commissioning and Training
Scott Thomson	Engineering Technology Lead	Engineering/Engineering Technology
Gary Kloster	Technical Baseline Manager	Engineering/Engineering Technology
Ken Gibson	Safety and Licensing Engineer	ES&H/Regulatory Safety

Note: The need to establish this team, selection of appropriate chairperson, and determination of scope of discipline involvement was confirmed at the PMT meeting held on August 15, 2001

3.1.2 Implementing Standards Selection Criteria

When properly implemented, the set of standards for will:

1 Provide adequate safety
2 Comply with applicable laws and regulations
3 Conform with the Top-Level Safety Standards and Principles

At a minimum, the assessment team also considered the following contractual [Ref. 1] requirements for the radiological, nuclear, and process safety as excerpted from the contract Statement of Work, Section C, Standard 7, Item (2):

> (i) The Contractor shall develop and implement an integrated standards-based safety management program to ensure that radiological, nuclear, and process safety requirements are defined, implemented, and maintained. Radiological, nuclear, and process safety requirements shall be adapted to the specific hazards associated with the Contractor's WTP activities.
>
> (ii) The Contractor's integrated standards-based safety management program shall be developed to comply with the specific nuclear safety regulations defined in the effective rules of the 10 CFR 800 series of nuclear safety requirements and with the regulatory program established in the following four documents:
>
> (A) DOE/RL-96-0003, *DOE Process for Radiological, Nuclear, and Process Safety Regulation of the RPP Waste Treatment Plant Contractor*;

(B) DOE/RL-96-0004, *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for the RPP Waste Treatment Plant Contractor*;

(C) DOE/RL-96-0005, *Concept of the DOE Process for Radiological, Nuclear, and Process Safety Regulation of the RPP Waste Treatment Plant Contractor;* and

(D) DOE/RL-96-0006, *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for the RPP Waste Treatment Plant Contractor.*

Changes to the four documents will be analyzed under RL/REG-98-14, *Regulatory Unit Position on New Safety Information and Back-fits*, and, if implemented, dispositioned in accordance with the Section I Clause entitled, *Changes*.

The integrated standards-based safety management program shall integrate the appropriate planning and practices elements specified in 29 CFR 1910.119, *Occupational Safety and Health Act of 1970, Process Safety Management of Highly Hazardous Chemicals*, to the extent that highly hazardous chemicals are present in quantities covered by 29 CFR 1910.119.

(iii) (only applicable to the Integrated Safety Management Plan)

(iv) The Contractor shall prepare and submit to DOE for review and approval, the radiological, nuclear, and process safety deliverables defined in Table S7-1, *Radiological, Nuclear, and Process Safety Deliverables.* Each deliverable is structured around the following six activities:

(A) Standards Approval;

(B) Initial Safety Evaluation;

(C) Authorization for Construction and Cold Commissioning;

(D) Authorization for Hot Commissioning;

(E) Oversight Process Determination; and

(F) Deactivation Safety Assessment.

3.2 Results of ISM Team Standards Selection Process

The ISM team reviewed a strawman update to Appendix A and B line by line for consistency and correction and developed the following proposed changes that are necessary as described below:

For SRD Volume I – cancel in its entirety. Previous revisions will exist for historical purposes.
For SRD Safety Criterion 3.1-7 replace the implementing standard ISMP 3.3.3, *Changes to Safety Documentation* and ISMP 5.6.2, *Updating of the Hazard Analysis Report* with 24590-WTP-SRD-ESH-01-001, Appendix A*, Implementing Standard for Safety Standards and Requirements Identification.*

The following change is proposed for SRD Safety Criteria (SC) 4.4-5, 4.4-9, 4.4-13, and 4.4-18, all revision 0: at the end of the first paragraph of each safety criteria delete "assuming a single failure." In addition, for SC 4.4-5 the sentence "The use of alternate equipment may be considered to satisfy the single failure requirement" is deleted.

The following changes are proposed for SRD Volume II, Appendix A, revision 0:

1 Add requirements for evaluation of chemical and direct radiation hazards.

2 Change the format of the standard to more closely follow the sequential steps of the ISM process.

3 Revise the presentation of common mode and common cause failures.

4 Delete the requirement that controls for SL-2 events satisfy the single failure criteria.

5 Replace details on SSC classification and quality attributes with references to SRD SC 1.0-8 and the QAP.

6 Includes editorial and wording changes to more clearly describe the standards selection process. A detailed identification of each proposed change for Appendix A is included in the attached Table 1.

7 Add new section 11.0, Maintenance of the SRD. Change Sections 11.0 and 12.0 to 12.0 and 13.0 respectively.

8 Add new figure 1, SRD Compliance Process.

The following changes are proposed for SRD Volume II, Appendix B, and revision 0:

1 Add requirements for evaluation of chemical and direct radiation hazards.

2 Delete the requirement to apply the single failure criteria to active SSCs required to achieve defense in depth.

3 Limit the application of the single failure criteria for SL-1 events to active (as opposed to active and passive) prevention and mitigation controls.

4 Delete the constraint that credit not be taken for tertiary confinement. A detailed identification of each proposed change for Appendix B is included in the attached Table 2.

For SRD Volume II, Appendix D, revision 0 it is proposed to revision section 2.0, seventh paragraph, 2nd sentence to "The binning process assigns postulated events to a certain severity level for further detailed analysis and comparison to Radiation Exposure Standards and Risk Goals.

The following change is proposed for ISMP Section 3.1, revision 6: Section 3.1.1 will be deleted entirely and Section 3.1 will include the following single sentence "Application of defense-in-depth for the RPP-WTP is provided in Safety Requirements Document (SRD) Volume II, Appendix B, "Implementing Standard for Defense in Depth."

For ISMP Sections 3.6.3 and 3.7.1 it is proposed to reference SRD Volume II, Appendix A instead of ISMP Section 3.1, "Defense-in-Depth".

For ISMP Section 3.7 it is proposed to delete the reference to SRD Volume I, Section 3.4.2 and add the sentence from SRD Volume I, Section 3.4.2.
For ISMP Section 4.2 it is proposed to delete the second paragraph in its entirety.

For ISMP Section 7.4 it is proposed to reference SRD Volume II, Appendix A instead of SRD Volume I, Section 3.6, "SRD Maintenance".

3.2.1 Adequate Safety

Canceling SRD Volume I, modifying the SRD Volume II, Appendices A, B, and D, revising the affected safety criteria, and modifying the ISMP to remain consistent is safe and does not impact the regulatory basis of DOE/RL-96-0004 and DOE/RL-96-0006 for the standard selection process or defense in depth. Justification for specific proposed changes is provided below:

1 **It is proposed to cancel SRD Volume I and move section 3.6, SRD Maintenance to SRD Volume II as Section 11.0.** SRD Volume I (except for section 3.6) contains only historical and duplicative information that is now identified in SRD Volume II, Appendix A, *Implementing Standard for Safety Standards and Requirements Identification*. The historical information will be retained in earlier SRD revisions. The information contained in SRD Volume I, Appendices A, B, C, D & E is no

longer current and has not been updated. The Standards Identification Process Database (SIPD) will provide the link for design requirements.

2 **It is proposed to "Limit the application of the single failure criteria to SL-2 controls as necessary to meet the target frequency.**" This is consistent with Appendix B Table 1, which states that for SL-2 events, "The single failure criteria shall be considered." However, the wording in Section 5.1 of Appendix A that "SSCs in control strategies for SL-2 events should satisfy the single failure criteria in the Implementing Standard for Defense in Depth" could be interpreted as imposing the single failure criteria on SL-2 events.

3 **It is proposed "That the application of single failure criteria is required to be applied to active systems and components only and not passive SSCs."** The application of the single failure criteria on passive components is more appropriate to nuclear plants during long term cooling (after transfer of emergency core cooling from the external tanks to the containment sumps [PWRs] or the wetwell [BWRs]). In these cases passive failures such as failures of pump seals and valve packing can result in a loss of recirculating fluid outside containment. Note that this does not relieve ISM Teams from considering passive failures (such as seal and valve packing leaks and piping and vessel failures) as initiating events.

4 **It is proposed to "Allow for credit for tertiary confinement when it is designed, constructed, operated, and maintained to appropriate standards."** There is no particular reason to allow credit for primary and secondary confinement but not tertiary confinement if the latter satisfies appropriate standards. Tertiary confinement can be affective in reducing radiological exposure for collocated workers.

5 It is proposed "That the application of the single failure criteria not be arbitrarily imposed on the Safety Design Class systems addressed by SC 4.4-5, 4.4-9, 4.4-13, and 4.4-18." Application of the single failure criteria should be a function of the severity level of the most limiting event for which the system is serving to prevent or mitigate.

3.2.2 Compliance with Applicable Laws and Regulations

The proposed changes do not impact commitments made relative to laws and regulations (e.g., commitments made to 10CFR820, 830 and 835 are not impacted, also 10CFR1910.119 and 40CFR68 will be implemented if the facility exceeds threshold quantities) or top-level safety standards (in particular, commitments to DOE/RL-96-0004 and –0006 are retained).

3.2.3 Conformance to Top-Level Safety Standards

Top-level safety standards for the ISM Process are provided in DOE/RL-96-0006 [Ref. 3]. These "0006" standards related to the ISM Process are identified as follows, along with an assessment of how use of the selected implementing standard ensures conformance to these top-level safety standards.

DOE/RL-96-0006; Item 5.2.2 Process Hazard Analysis

The Contractor should perform a process hazards analysis using acceptable industry practices. The process hazards analysis should be appropriated for the complexity of the process and the hazard. The Contractor should consider the effects of engineering and administrative controls, human factors, facility siting, and previous incidents in the hazard analysis. The Contractor should document the results of the hazards analysis including process hazards and possible safety and health effects. The Contractor should submit the results of the hazards analysis to the Director of the Regulatory Unit for evaluation and in support of authorization decisions and regulatory oversight.

One of the purposes of the hazard analysis is to evaluate the adequacy of the design and operating procedures. The Contractor should establish a system to address the findings in order to assure that the equipment and procedures provide an adequate degree of protection against accidents.

The Contractor should review and update the hazard analysis periodically to assure that the process hazards analysis is consistent with the current process.

Evaluation: The commitment to perform a process hazards analysis remains as documenting in SRD Volume II, Appendix A. The changes proposed to SRD Volume II, Appendix do not remove this requirement. Commitments to DOE/RL-96-0004 relative to standards selection to achieve adequate safety are also retained.

3.2.4 Evaluation Against Applicable SRD Safety Criteria

SRD safety criteria 3.1-7, relating to process hazard analysis, addresses the requirements for the process hazard analysis to be updated with the annual update of the FSAR. Since revising the implementing standard to SRD Volume II, Appendix A does not change this requirement, there is no impact from this change. The selected implementing standard meets these safety criteria.

4 Conclusions

The ISM Team determined that the proposed changes to SRD Volume II, Appendices A, B and D and Safety Criteria 3.1-7, 4.4-5, 4.4-9, 4.4-13, and 4.4-18 and the ISMP in addition to the cancellation of SRD Volume I continues to provide adequate safety, complies with applicable laws and regulations, and conforms to the Top-Level Safety Standards and Principles.

5 Recommendations

The proposed changes to SRD Volume II, Appendix A, B & D, Safety Criteria 3.1-7, 4.4-5, 4.4-9, 4.4-13, and 4.4-18 and the ISMP in addition to the cancellation of SRD Volume I should be recommended by the Process Management Team to the Project Safety Committee for confirmation.

6 References

1 DOE Contract DE-AC27-01RV14136, December 2000, US Department of Energy, Office of River Protection, Richland, Washington

2 *Safety Requirements Document*, 24590-WTP-SRD-ESH-01-001-02, Revision 0, Bechtel National, Inc., Richland, Washington. (Revision 0 issued September 2001).

3 *Top-level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006, Revision 1, July 1998, US Department of Energy, Richland Operations Office, Richland, Washington.

4 *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards, and Requirements for TWRS Privatization,* DOE/RL-96-0004, Revision 1, July 1998, US Department of Energy, Richland Operations Office, Richland, Washington.

5 River Protection Project Waste Treatment Plant Project Procedure, K70P568, *Hazard Analysis, Development of Hazard Control Strategies, and Identification of Standards*, Revision 0, 5 February 2001.